BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER
JUN 0 9 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	William B. Sweet et al.	Examiner:	Jeffrey D. Popham
Serial No.:	09/930,029	Art Unit:	2137
Filed:	August 14, 2001	Docket No.:	055120-0002
Title:	METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT		

DECLARATION OF PRIOR INVENTION UNDER 37 C.F.R. § 1.131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

We declare as follows:

1. We are the inventors of the subject patent application filed on August 13, 2001 and referencing provisional application No. 60/225,796 filed Aug. 15, 2000 and provisional application No. 60/239,019 filed Oct. 4, 2000. At the time the patent application was filed, we were employees of ULogon.com/ViaQuo Corporation which was subsequently combined with SiVault Corporation, the current assignee of the subject application.

2. This Declaration is submitted to establish prior invention of the subject matter of the present patent application in the United States.

3. Prior to the effective date of the reference Berson et al. June 19, 2000 (the filing date of the U.S. Patent No. 6,754,821 to Berson et al.) we conceived of our invention and diligently worked toward constructively reducing our invention to practice by filing U.S. Application No. 09/930,029 on August 14, 2001.

4. Exhibit A (71 pages) includes a copy of the provisional patent application filed October 4, 2000 in the USPTO. As evidence a conception date prior to this filing date, pages 3-15 and 17-55 refer back to June 28, 2000 while page 16 refers back to an even earlier date of May 20, 2000.

5. Exhibit B (40 pages) includes a copy of a disclosure document prepared internally at ULogin/ViaQuo Corporation and dated May 20, 2000. This disclosure/presentation document contains essentially the same material as that filed in the provisional patent application in Exhibit A. In particular, page 1 in Exhibit B includes the identical figure as page 16 in Exhibit A with the common date of May 20, 2000 thus

providing a conception date at least as early as May 20, 2000. The rest of this document is also dated May 20, 2000 thus indicating a conception date at least as early as May 20, 2000.

6. Following our conception prior to the critical date of June 19, 2000, we worked diligently with our Patent Attorney to prepare the provisional patent application filed on August 15, 2000, another provisional application filed October 4, 2000 and a non-provisional application filed August 14, 2001 thereby constructively reducing the invention to practice. During this time period, the patent attorney prepared one or more drafts of the applications for our comments. With our comments, the patent attorney revised one or more portions of the application, claims and/or figures to accommodate our suggestions.

7. At the time of preparing the content used in Exhibit A and Exhibit B prior to June 19, 2000, we had conceived of a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, the method comprising: (a) receiving a request for an access permission security profile on behalf of a network user; (b) authenticating the request; (c) creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object; and (d) securely transmitting the access permission security profile to the network user over the network.

8. We also had conceived of a method for controlling access to a secured system, the method comprising: (a) selecting one or more portions of the system to be secured; (b) creating one or more groups of system users, said groups defining which users are to be allowed access to which secured portions of the system; (c) establishing one or more access codes for each group; (d) assigning the access codes to the secured portions of the system, wherein each access code is adapted to be combined with other components to form a key for controlling access to one or more secured portions of the system. (e) securing the access codes; and (f) distributing over a decentralized public network the secured access codes to users of the system who are to be allowed access to one or more of the selected portions of the system.

9. Additionally, we had conceived of a method for administering cryptographic capabilities over a decentralized public network to a plurality of network users, the method comprising: (a) identifying one or more groups of network users for defining which users are to be provided with cryptographic capabilities; (b) creating a member account for each

network user in each group; (c) performing administrative tasks associated with maintaining the member accounts in a single database; (d) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; (e) creating one or more security profiles for each network user in each group, wherein each security profile is stored in the user's member account and contains at least one access code; (f) generating a member token relating to each security profile; (g) securing the security profiles and related member tokens; and (h) distributing the member tokens over the network to individual network users upon authenticated request and according to each individual user's security profile.

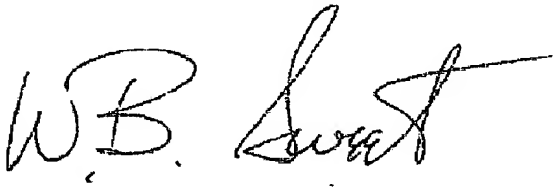
10. We further conceived of a centralized security management system for administering and distributing cryptographic capabilities over a decentralized public network, the system comprising: (a) a set of server systems; (b) a set of member domains, wherein each member domain is maintained on at least one of the server systems; (c) a set of system maintenance tasks associated with maintaining the set of member domains; (d) one or more system administrators for performing the set of system maintenance tasks; (e) a set of members, wherein each member is associated with at least one member domain via a member account; (f) a set of member security profiles, wherein each security profile is uniquely associated with a member account and provides cryptographic capabilities to the member associated with the member account; (g) a set of administrative tasks associated with maintaining the set of member accounts; and (h) a set of domain administrators for performing the administrative tasks remotely over the network.

11. We also conceived of a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, the system comprising: (a) a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network; (b) a set of server systems for managing the distribution of the member tokens; (c) means for requesting a member token from at least one server system; (d) a set of client systems, wherein each client system includes (i) means for receiving the requested member token, and (ii) means for utilizing the cryptographic capabilities provided by said member token; and (e) means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network.

14. All acts set forth herein and/or relied upon for the purpose of establishing invention prior to June 19, 2000 were carried out in the United States.

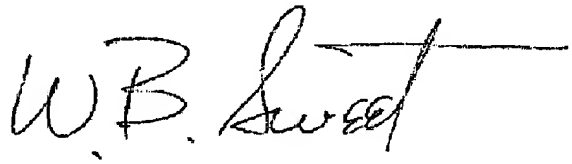
15. John J. Yu, the co-inventor of this case, cannot be found and is unavailable to sign the declaration herein below. We have attempted to locate him numerous times but have not yet been able to locate him. Several individuals he previously worked with indicated that he may have left to live in China however we cannot be certain and were unable to obtain contact information. Consequently, under MPEP 715.04 1 (d) William B. Sweet will be signing on behalf of Mr. John J. Yu as he is clearly a party in interest and has personal knowledge of the invention. (Parties available to make an affidavit or declaration under 37 CFR 1.131 include the assignee or other party in interest when it is not possible to produce the affidavit or declaration of the inventor. Ex parte Foster, 1903 C.D. 213, 105 O.G. 261 (Comm'r Pat. 1903))

16. We declare that all statements made herein are of our own knowledge and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.



_____ Date: June 8, 2006

William B. Sweet



_____ Date June 8, 2006

William B. Sweet on behalf of
John J. Yu

RECEIVED
CENTRAL FAX CENTER
JUN 0 9 2006

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Exhibit A: Provisional Application 60/225,796 filed August 15, 2000

Please type a plus sign (+) inside this box → +

Docket Number: 055120-0002

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Large Entity)

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle (if any))	Family Name or Surname	Residence (City and either State or Foreign Country)
William B. John J.	Sweet Yu	Morgan Hill, California Milpitas, California

☐ Additional inventors are being named on page 2 attached hereto

TITLE OF THE INVENTION (280 characters max)

Web-Based Application Service Model for Security Management

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number → Place Customer Number Bar Code Label here

OR

☒ Firm or Individual Name	Ronald S. Laurie, Esq.				
Address	Skadden, Arps, Slate, Meagher & Flom LLP				
Address	525 University Avenue				
City	Palo Alto	State	CA	ZIP	94301
Country	U.S.A.	Telephone	(650) 470-4500	Fax	(650) 470-4570

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification	Number of Pages	49	Drawings: A Technology Brief pp. 1, 19, 38 & 39, 14 sheets of slides, 2 sheets of figures = 20 sheets	
☒ Drawing(s)	Number of Sheets	20	☐ Other (specify)	

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

		FILING FEE AMOUNT
X	A check or money order is enclosed to cover the filing fees	
☒	The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 19-2385	$150.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE Ronald S Laurie DATE August 15, 2000

TYPED or PRINTED NAME Ronald S. Laurie, Esq. REGISTRATION NO. (if appropriate) 25,431

TELEPHONE (650) 470-4600

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

(Page 1 of 2)

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Large Entity)

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (city and either State or Foreign Country)

Certificate of Mailing by Express Mail Express Mail Label No. EL 441 850 674 US

I certify that this provisional patent application cover sheet, provisional patent application and fee is being deposited on Aug. 15, 2000 with the U.S. Postal Service as "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Jan Steele

Typed or Printed Name of Person Mailing Correspondence

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

[Page 2 of 2]

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Web-Based Application Service Model for Security Management

I. Executive Summary — June 28, 2000

ULogon.com's ("ViaQuo" is the new suggested company name) primary mission is:

Enabling Internet users to virtually be anywhere from anywhere, at any time, securely—and to have easy access to only the information they are entitled to

The Internet has become an essential means of information access and resource sharing. It relies on a simple, intuitive web interface for moving information instantaneously from one area to another. Although networking technology allows people to move information rapidly, it has not solved the problem of ensuring the right people get access to the right information from anywhere, while denying it to the wrong people. If a truly secure and manageable way were available, could we not literally make all our databases available from the web?

To solve this problem, ULogon came up with a radical concept: provide an Internet delivery channel that can move people (virtually) and information anywhere, and unite it with a system for managing information access securely, easily and across boundaries between companies. Airtight business-to-business information exchange, rich interactive experiences and personally rewarding online activities would be made possible by a system with a set of delivery tools that can support both extensive virtual people movement, as well as secure, fine-grained information access controls.

ULogon has segmented these capabilities into two categories:

1. **Virtual Presence** ("ViaPortal" is the new suggested name). Using Internet connectivity to allow remote control of and interaction with computer systems from great distances. This category includes remote monitor viewing, remote control of the target mouse and keyboard, bi-directional file transfer capabilities, the means to interact with other computer users via keyboard chatting and screen sharing, and ultimately the ability to interact via audio and video conferencing over the web. Virtual presence allows us to "be there" in every sense, short of kicking the computer when it fails.
2. **Secure Virtual Access** ("ViaSecure" is the new suggested name). Today there are major security obstacles related to the dissemination of valuable (but sensitive) information to employees, partners, customers, and vendors over the web. How can information flow easily to the right people, without flowing to the wrong people? ULogon solves this problem with Secure Virtual Access service, which depends on two radical new technologies. The first is Constructive Key Management[1] or CKM[1], which uses a new fine-grained access control technology for securely distributing information over the Internet[1]. The second is called biometric authentication technology (BioID[2]) that positively identifies users over the Internet[2]. By combining these authentication and access control technologies, ULogon can deliver a secure virtual access capability to companies that need to distribute and receive proprietary intellectual property over the Internet to a very broad spectrum of users both inside and outside the company.

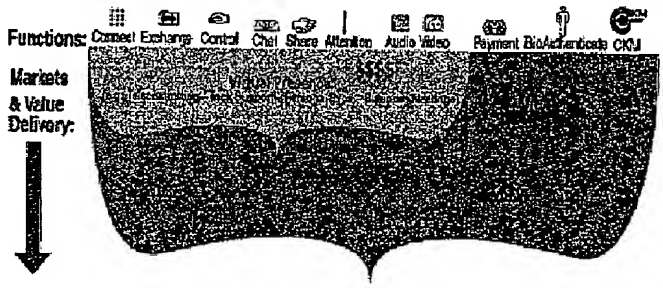
The mapping of ULogon's services and some suggested markets for those services is shown below:

---

[1] Constructive Key Management and CKM are registered trademarks of TBCSHC, Inc.

[2] BioID is a registered trademark of Dialog Computer Systems

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



A comparison of ULogon functions with anticipated applications

Examples of ULogon's service benefits to users include:

- Remote Access/Control—convenience, time savings, and remote access to office, home & Internet appliances
- Technical Support/Business Development (collaborating, sharing & meetings)—Faster resolution, lower cost, and highly personalized services

Examples of ULogon's benefits to business partners include:

- ISPs—new value-added services to offer new or existing customers
- Corporations needing a secure way to provision resources over the Internet—Increase in employee productivity by making any information ultra-accessible—quickly, inexpensively, without risk of damage, loss or exposure; plus the ability to spawn new customer services.
- Application Service Providers (ASPs)—new revenue opportunities from richer services incorporating heightened interactivity and better security
- Complex (e.g., distance education) content Providers—new delivery channels for their content

The first set of ULogon.com services will be the initial features of the Virtual Presence tools, which are currently being tested, with commercial service planned for September of 2000. The initial goal is to establish a customer base by providing value-added virtual presence services in order to prove the service model. We will then add Secure Virtual Access services when they become available early in 2001. At present, we are actively seeking strategic partners to license our technology and take it to market.

ULogon is still a very young company. It is currently looking for a second round of funding (approximately $5 million), to be used to develop the management team, hire additional employees and substantially advance product development (SVA and additional VP features) as well as to build an ultra secure, high volume web site for managing connection profiles for millions of users and businesses.

II. Market

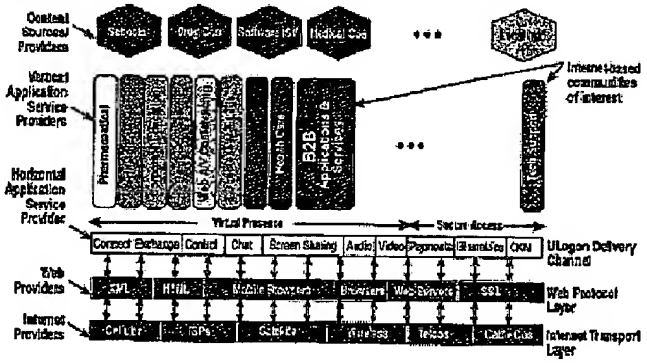
Market Opportunity

A drastic reduction in the cost of computer hardware, along with an explosion in the Internet bandwidth is driving the creation of a new generation of interactive services delivered over the Internet. Stand-alone hardware and software sales are being supplanted by application service provision over the Internet. Companies are under obvious competitive pressures to migrate their businesses to the web and create new e-businesses. At the same time, they must protect themselves from the inherent security exposures of doing so. Organizations are faced with the challenge of making appropriate information to customers, employees and partners flow freely, while balancing security issues.

The timing of these trends presents a unique opportunity to create a horizontal application delivery layer and/or Application Programming Interface that allows companies (or the ASPs serving them) to guarantee

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

the secure provision of internal company data to employees and business partners, as well as external service content delivery to customers, regardless of time or physical proximity. A reliable, cryptographically secure data transmission layer including transactional auditing tools is required to enable a host of next generation high-end services.



ULogon intends to provide a value delivery channel to the Internet market

The market requires an information transmission layer be in place to securely deliver and transact vast amounts of information to millions of consumers and businesses. The first of these segments is the creation of virtual presence services capable of allowing people to interact with computer assets and other users in real time, without regard to physical proximity. The next segment requires authentication, encryption and user credential management layer to ensure high information dissemination security. As the information revolution unleashes the service provision of vast amounts of intellectual property across the planet, the virtual presence and secure virtual access tools need to be in place to reduce the physical and security barriers to making information and e-services a truly pervasive part of the information economy.

Customers/Partners/Competitors

The market is currently characterized by a collection of companies that could easily be customers, partners or competitors of ULogon's anticipated services:

1. Remote access software vendors selling a subset of virtual presence software products over the web or dialup environments (goAnywhere, Timbuktu, LapLink). These are clear competitors for our virtual presence products. ULogon's Virtual Presence product is better in two ways: (a) all of their products require a client piece of software be installed on both the remote and target machines in order to work; and (b) the software must be purchased up front for between $89 and $149/seat (ULogon's service costs only a few dollars per month to "rent."). A key capability of the ULogon product is that it only needs client software installed at the target end; any Internet-connected computer with a browser can be a viewing machine. This allows "thin client" systems to remotely control much larger and more sophisticated target machines, and offers an added dimension of utility for the coming "webpads."
2. Internet Service Providers of all kinds, both domestically and internationally. These companies are potential customers for ULogon services, and could either outsource (ULogon-powered link on their site) or license the capability. It is anticipated that in many foreign markets, licensing is the preferred approach, due to poor connections or low bandwidth among the various countries. At present, with little selling effort, ULogon has set up beta testing arrangements with an ISP in Australia and another in Singapore—both of whom want to include Virtual Presence services as a free part of their basic services to over 400,000 subscribers (at $1–$2/month/user to ULogon).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

3. Web-based personal file transfer and remote operations vendors (uRoam, Relm, eTunnels). These are direct competitors for the low end of Ulogon's virtual presence services. At the moment, all are lacking full remote control capability, but it is likely that they will evolve to provide it. None possess the secure virtual access features we will offer. It is unlikely that these companies will license or outsource ULogon virtual presence services, although they may very well license the secure access services.
4. Web-based conferencing vendors [business meetings] (Webex, Placeware). These are competitors for the high end of Ulogon's Virtual Presence services. None possess the security management technologies we intend to offer. It is unlikely that these companies will license or outsource ULogon virtual presence services, although they may very well license the secure access services.
5. eLearning sites providing horizontal content and vertical services (Blackboard, Click2Learn, Convene.com, DigitalThink, Docent, Giliat Communications, Hungry Minds, Integrity Training, KnowledgePlanet, Lotus, Netg, Net-Learning, New Horizons, Pathline Software, PeopleSoft, Saba Software, Skillsoft, SmartForce, SmanPlanet, TeamScape, WBT Systems, etc.). All of these companies are potential customers (resellers) of ULogon services in the distance learning market, especially the secure virtual access service.
6. Web-based Business Exchanges (Agile Software, Ariba, Commerce One, FreeMarkets, i2 Technologies, Oracle, PeopleSoft, PurchasePro, VerticalNet, and Vitria). All of these companies are potential customers (resellers) of ULogon services in the business-to-business exchange market.
7. Web-based Customer/Partner Relationship Management (CRM/PRM) (Allegis, Bowstreet, ChannelWave, Clarify, Click Interactive, Drums, Epiphany, Eprise, Front Line Solutions, Intelle, NetPCS, Onyx, Oracle, Partnerware, Pivotal, Radnet, SalesLogix, Siebel, Supply Search, Ten North, Vantive, Webridge, etc.). All of these companies are potential customers (resellers) of ULogon services in the customer or partner relationship market.
8. Other Internet Application Service Providers (ASPs) including Applicast, AristaSoft, BrightStar Technology Information Group, Corio, CyTex, eALITY, ebaseOne Corp., EDS, Eggrock, eOnline Inc, FutureLink Distribution Corp., IBM Global Services, Interliant, Interpath Communications, Learning Station.com, NavISite, Oracle Business Online, QSP Inc., Qwest CyberSolutions, Telecomputing, The TriZetto Group Inc., USinternetworking, and World Technology Services. All of these companies are potential resellers of ULogon services in their respective ASP markets.
9. Other direct corporate groupings that may need Virtual Presence, and/or Secure Virtual Access services include:
   - Governmental-oriented Systems Integrators & contractors (Boeing, General Dynamics, Lockheed Martin, Raytheon, Rockwell Collins, Northrop Grumman, General Electric, Hughes, Raytheon, United Technologies, Space Systems/Loral, Aerojet, etc.)
   - Database management companies (Oracle, Sybase, SAP, PeopleSoft, Ingres, TRW, Informix, Cincom Systems, etc.)
   - Commercially-oriented Systems Integrators and consultants (Arthur Anderson, KPMG, Booz-Allen & Hamilton, Deloitte Touch, Ernst & Young, etc.)
   - Major corporations with huge databases of Intellectual Property (e.g., Pharmaceutical—Abbott Labs, Eli Lilly, Bayer, Bristol Myers Squibb, Ciba-Geigy, Glaxo-Welcome, Hoechst, Merck, Parke-Davis, Pfizer, Roche, Schering-Plough, SmithKline Beecham, Warner Lambert)
   - Insurance companies, especially those in health care (Aetna, CIGNA, Kaiser Permanente, Landmark Healthcare, Blue Cross/Blue Shield, Humana, Prudential Healthcare, etc.)
   - U.S Government Agencies requiring CKM systems, but unable to obtain sufficient smart cards (at present the Department of the Interior wants 10 million CKM seats next year—more on this later.)

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Market Potential

There are a number of markets for ULogon technology, and one of the best is pharmaceutical dispensing. Two pharmaceutical companies we are talking to would like to use the Internet in new ways to substantially improve their communications capability with customers and employees. They want to be able to use the Internet to directly communicate to—and receive confidential information from—people participating in drug trials, as well as chronic drug users. (They will thus minimize the traditional role of doctors in collecting and disseminating information) They also want to "vend" drugs to these people through a "pill-dispensing" Internet appliance. They are already building the Internet appliance, and are stumped at the problem of how to make sure the right information gets to the right people, while simultaneously guaranteeing that it won't get to the wrong people. They also need to be able to strongly authenticate their users, as well as interact with them and their computer systems. They are both very excited about the ULogon story. ULogon services would provide the following benefits:

1. Rapid implementation and scalability
2. Support for all legacy network topologies and requisite infrastructure investment
3. Effective electronic delivery certification and audit trail
4. Improved throughput, elimination of security bottlenecks and single points of failure
5. Allows all information files to be freely and safely placed on the web
6. Enhanced network authentication through advanced biometric technologies
7. Enables the creation of wholly new web-based products and services

The real benefit is that using these new services, a pharmaceutical company can increase the profits on their drug product lines by about $44 million each (for one of our customers with 100 drug lines, that translates to $4.4 billion.)—A goal that can easily justify the costs of the ULogon services.

But pharmaceutical companies are not an isolated case. Most major corporate web sites will need a way to scale their networks to tens or hundreds of millions of customers in the future, while creating and rolling out new services.

We are aggressively seeking feedback from a variety of customers that we think would benefit a great deal from what we provide. Thus, the precision of our measure of the true market potential will increase over time. Irrespective of this, we have made conservative revenue and market share assumptions that *still* demonstrate the huge potential we believe we can achieve.

Assumptions:

- We believe the ASP (Application Service Provider) market will represent a significant reseller base for our technology at the high end, especially for Secure Virtual Access services
- We believe that there is another market segment consisting of companies that need ULogon services to enable or enhance the direct selling of their custom products or services, using an ASP-like model. In effect, ASPs sell (rent) *new* information-based products or services over the Internet, whereas the Direct Corporate segment ULogon believes is out there uses web-centric services to sell more *traditional* products (such as health care, software, drugs and distance education). Although we have not found summary market research data on this market segment at present, we believe it is at least as large as the ASP segment. As examples, IDC reports the following market size estimates for applications that fit this definition:
  - U.S. Corporate distance education will reach $7.1 billion by 2002;
  - WW information technology training & education will reach $27.9 billion by 2001;
  - Software tech support market will reach $42 billion by 2003;
  - Network tech support will reach $8.8 billion by 2003
- We believe the ISP (Internet Service Provider) market will represent a significant reseller base for our technology at the low end, especially for Virtual Presence services that they can offer as premium services incremental to their basic connectivity services.
- We assume that "WebCKM"-based secure access service can be sold as a percentage of the value of an ASP service, where that value may represent approximately five percent of the total value of an ASP implementation. (The alternative is to sell it for a monthly fee/seat.)

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 12 of 115

- We believe that Virtual Presence services will be sold on a monthly fee/subscriber basis, for $.50-$8/month, depending upon the feature set used.
- We assume 6% ASP market adoption of CKM in two years, with little direct competition for web-based CKM service due to CKM's newness and the fact that no one else is currently contemplating a web-based CKM offering. WebCKM should sell for $5-$12/month/user.
- We assume a slow adoption rate for the audio/video portion of our virtual presence (interactivity) products, due to bandwidth limitation of the "last mile" (only 3% of homes have high bandwidth connections). By 2003 this problem will have eased substantially due to the rapid growth in high bandwidth internet connections (IDC forecasts that 33% of Internet-connected homes will have high bandwidth connections by then).
- At present, we do not assume any U.S. Government CKM business, but that assumption is changing rapidly due to a production bottleneck in smart card availability.

Application Service Provider market numbers. IDC projects 1999 ASP revenues will be $296 million, climbing to $7.8 billion by 2004 (a 92% CAGR). Dataquest projects 2003 ASP revenue to be $22.7 billion (a 91% CAGR). If we assume the true value of the market is an average between these two projections, a third set of numbers can be created:

Taking into account the above assumptions, we believe we can achieve in excess of a $100 million/year

ASP Market Growth (IDC)

Revenues in Millions of Dollars

	1999	2000	2001	2002	2003	2004	CAGR
Total Spending	$ 296	$ 628	$ 1,295	$ 2,484	$ 4,627	$ 7,784	92.9%

ASP Market Growth (Dataquest)

Revenues in Millions of Dollars

Region	1999	2000	2001	2002	2003	2004	CAGR
North America	$ 398	$ 756	$ 1,452	$ 2,717	$ 5,154	$ 9777		89.7%
Europe	$ 293	$ 555	$ 1,051	$ 1,981	$ 3,770	$ 7,141		89.4%
Rest of World	$ 197	$ 387	$ 700	$ 1,492	$ 2,991	$ 5,757		98.4%
Grand Total	$ 888	$ 1,697	$ 3,203	$ 6,190	$ 11,836	$ 22,675		91.2%

ASP Market Growth (IDC & Dataquest)

Revenues in Millions of Dollars

	1999	2000	2001	2002	2003	2004	CAGR
Total Spending	$ 1,184	$ 2,373	$ 4,265	$ 8,253	$ 16,090	$ 30,693	92.0%

business within three years. These assumptions are conservative when considering the value, novelty and lack of acceptable alternatives to CKM, which is the crown jewel of the ULogon service offering.

III. Technology

Virtual Presence

ULogon.com has developed two innovative technologies to provide Virtual Presence services.

1. The first is an HTTPS-based certification issuance and access session setup system (patent pending) which enables the dynamic remote host (TCP/IP addresses) to URL mapping. This is a key technology that enables the central location for user authentication and connections profiles. It simplifies creating a virtual network over the Internet for all individuals and businesses (reducing or eliminating the need to hire system administrators).
2. The second technology is a pure web-based remote operation and control client and server system that allows the user to remotely execute applications, see their desktop, and view files without have to download it across the Internet. It is a thin client running within any browser such as Microsoft Internet Explorer or Netscape Navigator.

Audio/Video. ULogon will build its own application sharing and keyboard chatting functions on top of its present remote control functionality within the next three months. We were planning on evaluating audio/video technology sources with the view of selecting the best one for our future interactivity services. However, given the enthusiastic reception we are now experiencing over WebCKM in our talks with potential customers, the interactive audio and video services will be put on hold status until the Secured Virtual Access ("WebCKM") service is ready for beta testing early next year. At that point we will assess the potential for audio and video services—and the impact they may have on our resources—and make a

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 13 of 115

decision accordingly. (Our original plan was to obtain a tunable technology that automatically reduces the quality of the audio/video signal, depending upon the Internet bandwidth available to the user's system. One option is to license the appropriate technology from an existing vendor such as CUSeeMe (White Pines Software) and then design and build our own special technology after gaining market experience and a customer base. It is expected that DSL or cable modems will deliver sufficient bandwidth to provide one or two reasonably large video windows running at 10-30 frames per second with high quality sound.)

Secure Virtual Access

To provide Secure Virtual Access, two new technologies will be needed: biometric authentication and Constructive Key Management.

Biometric Authentication. A new technology called BioID is now available that recognizes people through face, voice, and lip movement using a PC-based camera and microphone. To authenticate themselves, users look at the camera and speak a pre-registered "pass-phrase" detected by a microphone. A static picture of the person's face is taken and processed to recognize facial characteristics, relative to a pre-registered template of the person's face taken during enrollment. In like fashion, the person's voice speaking the pass-phrase is also transformed into a template and compared to the enrollment version, as are the lip movements speaking the pass-phrase. This technology allows customers to select combinations from three different modes of biometric authentication. One mode may be used for low assurance applications; two modes may be used for higher assurance applications, and for situations where one of the modes is not operating properly due to a change in facial or voice characteristics. All three can be required for the highest assurance applications. One big advantage of this technology is the ease of enrollment. People can be enrolled (initially registered) easily over the Internet, since the characteristics normally used by human senses are the same ones used by the digital authentication technology. People can be interviewed live over the Internet, and can even hold up their driver's licenses or passports to the camera for picture ID purposes.

Constructive Key Management (CKM). The computing industry is selling a trillion dollars worth of computers, networks and software every year so that corporations and government agencies can store, retrieve and process corporate information of one kind or another. Today, companies wishing to migrate to a complete electronic enterprise face a major hurdle: how to make their most valuable information available to employees, partners, customers and suppliers—with the associated audit trails of responsibility and accountability—while ensuring each constituency only obtains what they are properly authorized to. Modern cryptography can provide answers to the problems of information privacy, user authentication, and user non-repudiation, but it doesn't answer the question: should this person's request for a specific piece of information be granted? How can companies put their valuable intellectual property on the Internet in order to gain higher levels of productivity or sell new services, without the risk of loss, inappropriate use, or embarrassment?

Recently, an elegant solution was invented to solve this problem. The solution is called Constructive Key Management (CKM) and it brings three major advantages over traditional public key crypto infrastructures:

- **Decentralized operation.** CKM decentralizes the security processing by issuing each user his/her own set of credentials that control the creation of or access to encrypted information objects on the network. In a CKM system, all information content sits on the network in encrypted form. Each desktop system directly deposits or accesses the information over the network, and if the appropriate access permissions are in the user's credentials profile, he/she can create or "consume" the information. If not, the information is simply meaningless garbage. The CKM catchphrase is "secure the data, not the channel."
- **Fine-grained object architecture.** CKM allows dividing information files into smaller subsets called objects. In Microsoft Office, for example, anything that can be selected can be made into a separate object. Each object is separately symmetrically locked (encrypted) with its own unique working key, which is only unlockable (decrypted) via a set of credential keys pre-assigned at the time the object is created. Objects may be contained within objects and the whole object-oriented structure can easily map to the way in which information should ideally be shared within an organization. Since traditional public key infrastructure (PKI) systems can typically only encrypt or decrypt a complete file, this CKM fine-grained architecture is a substantial benefit to the information control process.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

ULogon Business Summary

- **Standardized credential architecture.** CKM credentials allow read, write or read/write access to data objects that can be subsets of a single file, document, picture, or database view. Credentials are pre-defined by a domain authority, and the credential subsets assigned to each user (member) are distributed and maintained by a workgroup administrator. Credentials are needed to both create and consume information, and since all objects are digitally signed by the creators, there is a certified audit trail of all information created within the system. This standardized mechanism for defining and maintaining credentials brings a very powerful, yet easy to maintain way of assigning, enforcing and managing creation and access permissions.

The current CKM technology implementation relies upon each member possessing a special CKM-enabled smart card, which holds the member's credentials, encryption keys, and the required crypto security protocols securely. Other CKM-enabled software resides on the desktop, and consists of the plug-in modules that enable the application of credentials on top of normal desktop applications (e.g., Microsoft Office) as well as the encryption/decryption operations to lock/unlock content and digitally sign/verify the content.

Currently, the US Postal Service is in the early stages of deploying a new CKM-based secure electronic email system (code name "NetPost.Certify") to companies that report mandatory data to selected federal agencies. TECSEC, Inc. the inventor of CKM, is responsible for building the CKM desktop and administrative software, and CryptTEC Systems (the company Franz Reasel and Bill Sweet previously helped to found) is working in partnership with TECSEC to supply the smart cards that the USPS requires.

Through this new certified email service, a corporation sending mandatory data to a Federal agency would do so via the Internet with the aid of an USPS smart card. All of these data transmissions can take place over the Internet as pieces of electronic mail—quickly, inexpensively, and securely. The first major customers for the service will be the IRS, the Social Security Administration and the Health Care Financing Administration, which processes Medicare/Medicaid data on behalf of 75 million Americans. Other federal agencies will follow over time. (The internal USPS forecast is for 100 million users over a 5-year period.)

Integrating BioID and CKM. ULogon plans to adapt the CKM technology to a web-centric model ("WebCKM") that uses a web server account for each user, such that the default mode of operations does *not* require a smart card or reader (but could easily operate with smart cards and readers if desired). Instead of accessing user's CKM profile (keys and credentials) on a smart card through a smart card reader driver, the desktop CKM software accesses the member's profile on a web server account maintained at a ULogon.com web site. This provides lower costs (e.g., $5–12/month instead of $125-$150 up front), rapid adoption, much higher convenience, and better security and mobility of users (assuming the BioID authentication). It also maintains the 2-factor security status that the government insists upon: instead of something you know (a PIN) and something you have (a smart card), WebCKM uses something you know (a PIN) and something you *are* (a biometric measurement).

CKM is an unknown technology in the commercial sector due to its relative newness and TECSEC's current focus on government customers and applications. However, ULogon sees CKM as a technology enabler for many corporate customers with large numbers of people needing easy differentiated access to millions of pieces of information. Using biometric authentication, employees, customers, suppliers, and others can be easily and positively authenticated to the ULogon central site, which will possess all of the credentials necessary for them to access or create the content desired:

1. Information creators can create intellectual property content and encrypt it in object groupings for encrypted storage on Internet-accessible servers. Only the people who possess the appropriate credentials on the ULogon web site will be able to access that content—and payment of the required fees (if any) can be one of the required credentials.
2. Corporate administrators can issue and update credentials via signed and encrypted files that are deposited in each member's account at the ULogon central site.
3. Members can create encrypted and digitally signed objects as they work, attend classes, or consume information via ULogon facilities online. This way, a person's participation in the process can be recorded and certified at each step of the process, saved electronically, and retrieved at any point in time to yield an audit trail of a person's work, study, or consumption history with the organization.

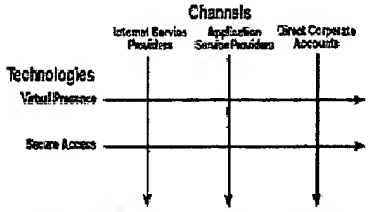
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 15 of 115

With the biocentric authentication and CKM-based signed and encrypted information objects, corporations and institutions will have substantially better control of the resource management process than the existing hodgepodge of electronic- and paper-based security processes.

IV. Business Strategy

At present, ULogon anticipates creating two major product service groupings that it will offer to several major application markets, utilizing three channels of distribution, as shown below:



From customer and partner contacts so far, ULogon has received a very enthusiastic response to the vision of providing a secure delivery channel for moving people and information over the Internet. However, the company has not had enough time or money to properly explore either the desired phasing of the development of interactivity and secure access capabilities on the one hand, or the most appropriate distribution channels on the other. More development and marketing resource needs to be expended to understand the intersections between technologies (capabilities) and channels shown above.

Business Models

The anticipated business models for ULogon are based upon collecting either monthly fees for different classes of web-based services (e.g., ISPs & corporate customers), or a percentage of the fee charged for the service (e.g., ASPs):

- **Virtual Presence—Remote Control.** It is anticipated that a registered virtual presence customer would pay between $.50 and $8.00 per month for the remote control portion of the service (Timbuktu costs $150/seat, PCAnywhere costs $80/seat), with approximately 50% of that revenue ($0.50–$4.00) coming to ULogon, and the balance going to the reseller (e.g., an ISP). (Two of our ISP customers anticipate giving away the service and paying ULogon between $1 and $2.50/user/month.)
- **Virtual Presence—Interactivity.** The ability to avoid the very measurable costs of transportation—either for attending a meeting or a class via the Internet—or the ability to offer better services such as tutoring and technical support, means that virtual interactivity has a much higher value to the user than remote control. ULogon anticipates a monthly fee from users of between $5 and $30 per month, with $3-$15 going to ULogon, and the balance going to ISPs, systems integrators and Internet ASPs providing the end service to users (Placeware charges $400/year for its virtual interactivity).
- **Secure Virtual Access.** TECSEC is currently charging $129/seat for CKM, implemented in a non-web-based system. The customer must also buy a smart card and reader for another $50. If he/she wants BioID, it will cost another $50/seat. These numbers are subject to discounts for large volume customers, and can go as low as $100-150/seat for very large customers such as government agencies and large corporations. ULogon anticipates charging between $5 and $12 per user per month, with a royalty going to both TECSEC and the biometric vendor (DCS) of approximately 25%. This would bring in between $3.75-$9/month to ULogon.
- **Alternative Models.** Alternatively, a package deal for Application Service Providers and distance learning companies would charge a % of the service fees collected (e.g., 5%).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

V. Current Exciting Opportunities

ULogon has only been actively selling the ULogon vision for the last three months—and then with only one person doing the bulk of the selling. However, our progress in these three months has been remarkable.

- **Virtual Presence.** ULogon has stayed away from most of the large U.S. ISPs because we were afraid we were not ready to turn them on. The fear was if we turned them on before we had the capability to deliver WebCKM, they might go elsewhere to obtain it. We focused instead on a small number of overseas ISPs that were not likely to either compete with us, or go around us if they became too excited to wait for us to deliver. Two of these—Highway One (Australia—100,000 subscribers) and StarHub (Singapore—300,000 subscribers) were very interested in our story and, after viewing a demo of the virtual presence capability, immediately began discussing giving away virtual presence services as a part of their ISP service to their customers. Both are now about to begin beta testing of the product and both are eager to offer WebCKM when it becomes available. We believe we can replicate this experience with many of the other 2500 ISPs around the world.

  A couple companies—Hallmark Cards, Traynor—are interested in using Virtual Presence to enable their employees to access large and sophisticated computer systems from smaller, cheaper "thin client" systems. Hallmark Cards, which has about 800 artists and over a hundred million pieces of artwork, currently has to supply each artist with a very sophisticated Macintosh computer with large memories and complex software. They are also worried about their artwork library being looted by their competition. They want to be able to hire artists that are part-time and/or remote to their office locations. They could set up a room full of sophisticated Macintosh machines in a secure location, and then allow their new artists to remotely control these machines on a time-share basis from their homes, using less expensive computers as viewing platforms. They will thus have fewer expensive computer systems to buy, and can reach more artists around the world. By turning off file exchange capabilities and using WebCKM, they can keep better control over their artwork library. Traynor is an architectural design company that wants to allow design teams to access large CAD files from all around the country without having to move the files and worry about synchronizing versions. We think there may be many other such remote-control-of-sophisticated-computers-by-thin-client-systems in the market—particularly in future wet pad applications.

- **Secure Virtual Presence.** A while back Franz Rassel opened a channel to Sprint headquarters through some mutual friends in Kansas City and pitched a few Sprint mid-level people on our vision. To our surprise, he got a highly enthusiastic reception and now, through a personal connection between our friends and the Sprint chairman, we are heading towards a demo and presentation to the higher levels early in July. This is both good and bad news: It is good because Sprint's new ION service—3 megabits download, 1 megabits upload, 4 phone lines and 750 minutes of long distance, all for only $100/month—is their preordere new weapon to take market share away from the likes of AT&T. They are currently rolling it out in Seattle, Dallas and Kansas City. Obviously, virtual presence services from ULogon are a nice service to bundle into ION. However, they see our planned WebCKM (Secure Virtual Access) as the really big differentiator for ION, one that would appeal to thousands of small to medium sized companies who want to get big company security capability at small company prices. It is bad because if it is important enough to them and we can't deliver in time, they may try to take the idea and implement it some other way.

  Another similar opportunity has now popped up via Franz's personal relationships from Bertelsmann (Germany), one of the top ISP/media companies in Europe, handling well over 10E million customer profiles. They are interested in both Virtual Presence and Secure Virtual Access services.

  ULogon plans to license the CKM technology and take it to the commercial market as an ASP Internet service. So far, we are the only company with this idea (equivalent to Verisign's plan to take RSA public key technology six years ago, when few people understood the impact potential of PKI). Our original plan was to take CKM to the commercial market as a web-based service, while TECSEC, the inventor of CKM, took it to the government market as a smart card-based product. (They have a 17-year contract with the USPS and a bunch of patents on the technology.) However, we are now being told by TECSEC that the smart card industry cannot produce enough smart cards for the government

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 17 of 115

programs (fab production limitations across the industry) and government agencies are likely to be willing to buy our web-based CKM service instead. The first such agency opportunity is the U.S. Department of the Interior, which early this month requested 10 million CKM seats to be delivered by early next year. When told that smart cards would not be available in such volumes, they immediately offered to take software instead, and the president of TECSEC called and asked if we could deliver WebCKM by early in 2001. Since it is likely that we would split the revenues with TECSEC, and since $5/month/member is a reasonable fee for such a high volume customer, ULogon and TECSEC could each be taking in $25 million/month in a year or two for just this one opportunity.

VI. Management Team

Bill Sweet, President. Mr. Sweet is an ex-electrical engineer and an ex-programmer who has held high marketing and sales positions with companies such as General Electric, Concurrent Computer, National Semiconductor, Zilog, General Automation, Atalla, Trusted Information Systems, and CrypTEC. Over the years, he has also become a crypto security expert and a high technology litigation expert witness, and operated a high technology consulting firm that numbered many Silicon Valley companies in its clientele. He builds good solid teams because he is very experienced in modern synergistic teambuilding, having developed and run his own teambuilding seminars for the last twenty years for a large number of clients. He has tutored hundreds of people in computer and cryptography sciences, and was a founder of CrypTEC Systems, a software development company specializing in secure smart card operating systems and applications. Bill holds a Bachelor of Science degree in electrical engineering and a Masters in industrial administration from Purdue University in West Lafayette, Indiana.

John Yu, co-founder, and CTO. Mr. Yu was also previously founder and vice president of technology at Advanced Communication Devices Corp. where his roles included engineering management and technology development in software and networking. Prior to that, Mr. Yu held various key technical positions at Silicon Graphics in the field of Internet, Java and web technology. Mr. Yu holds an MS and a BS degree in Electrical Engineering from the University of Tsinghua, China.

Ken Han, co-founder and VP Development. Prior to joining ULogon.com Mr. Han held the positions of key designer and project manager at Sun, Inc. Mr. Han also brings extensive experience in broadband communication technology, video conferencing, remote-access devices, and PC technology. He holds an MS and a BS degree in Electrical Engineering from the University of Tsinghua, China.

Franz Ressel, VP Business Development. Franz Ressel has 20 years experience in the high tech industry. He was educated in Graz, Austria in Industrial Electronics. He has designed and managed high tech projects for companies like Hallmark Card, Sony Electronics, PING Golf, and Celebrity Cruise Lines to name a few. Franz is the Co-Founder of CrypTEC System a Silicon Valley based smart card software company. He served as the early CEO and president, as well as the Vice President of Market Management for CrypTEC. Franz has extensive experience in electronic design, multimedia applications, and programming and international business development worldwide. Franz is a native of Austria and speaks fluent German.

A number of other senior staff members have been interviewed and are standing by waiting on this next round of funding before coming aboard. These include potential VP's of sales, marketing and finance.

Board of Directors

The ULogon Board of Directors consists of John Yu, Ken Han, David Liu, James Hsieh, and David Heaks. David Liu and James Hsieh are "angel" financial supporters of ULogon who made their money in high technology companies located in Boston, MA. David Heaks is the CIO for Alta Vista.

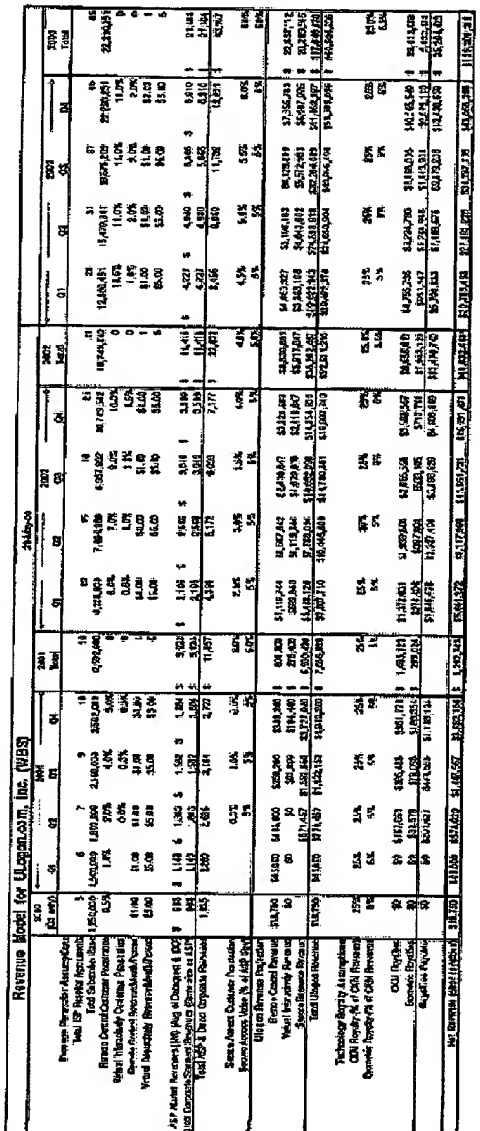
VI. Financials

The following financial P&L estimates are very tentative and are being shown as a rough estimate of the potential anticipated over the next three years. More detailed financial data will be supplied at a later date, after ULogon.com management and its financial advisors have had time to refine the data.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

ULogon Business Summary 6/28/00

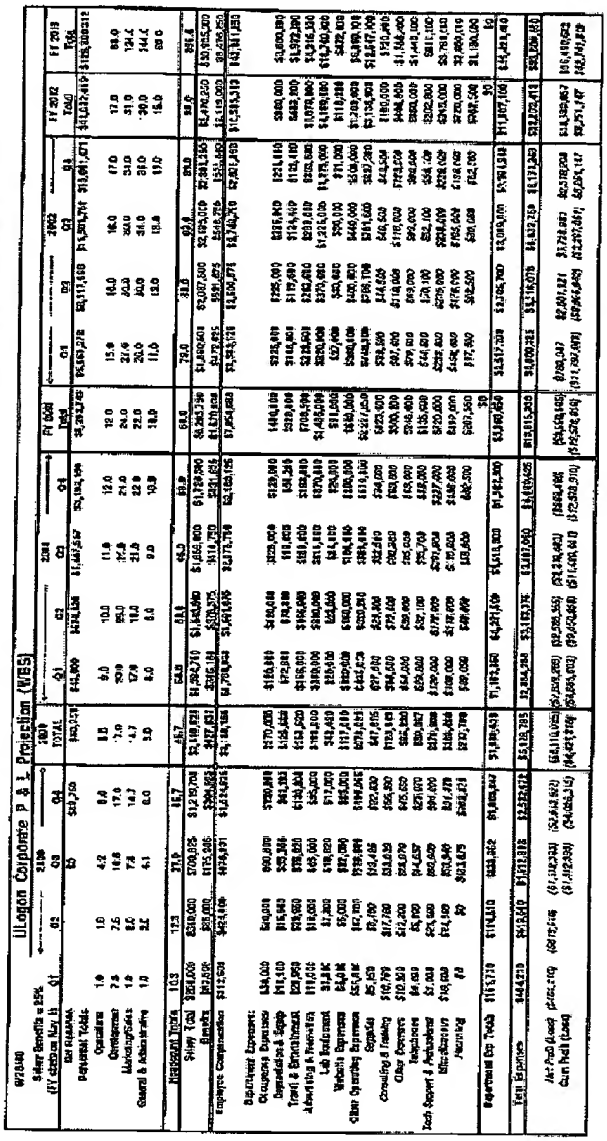
An estimate of the revenue potential and profit & loss projections for ULogon.com are as follows:



ULogon CONFIDENTIAL Page 12 6/28/00

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 19 of 115



ULogon Business Summary

ULogon Corporate P & L Projection (WBS)

6/28/00

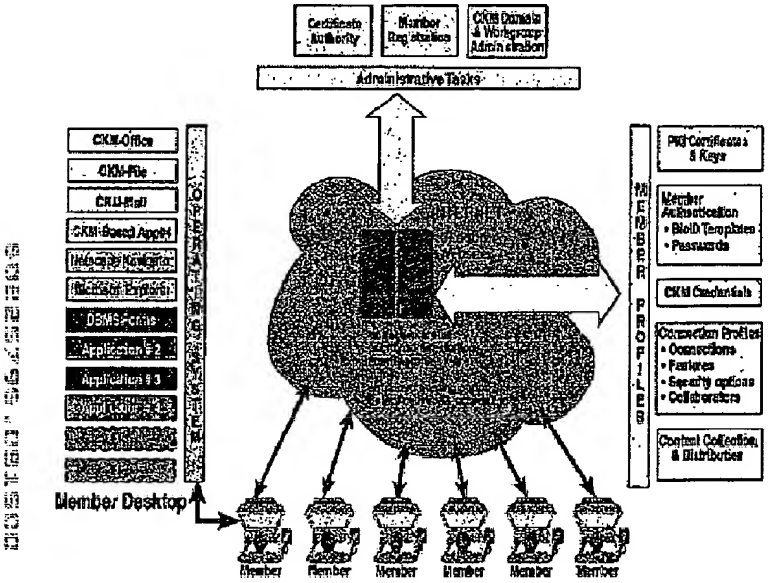
ULogon CONFIDENTIAL

Page 13

6/28/00

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

WebCKM:
A Technology Brief



VERSION 1.0 (5-20-00)

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

TECSEC® Incorporated
1953 Gallows Road, Suite 220, Vienna, VA 22182-3934
Tel: 703-506-9069 Fax: 703-506-1434
www.tecsec.com

Ulogon.com, Inc.
2460 N. First Street, San Jose, California 95131
Tel: 408-232-4858 Fax: 408-252-9210
www.ulogon.com

Table of Contents

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

1. Introduction

At present, the commercial electronic commerce world seems committed to public key-based (asymmetric) cryptography for its digital signature and key exchange needs, and symmetric cryptography for actual bulk encryption of information.

Public Key Infrastructures (PKIs) are very good for moving information from point A to point B securely, and for providing secure authentication and non-repudiation. However, modern PKI technology still does not completely satisfy the problem of properly accessing the information once it is safely in residence at point B. This is a particularly important problem for one critical class of users: large organizations such as government agencies, educational institutions and corporations, where thousands of users need instant access to millions of pieces of information—but where each person should only have access to the information to which he/she is entitled.

Consider this problem: a specific view (report) of selected data fields in a large database contains critical pieces of information that 208 people in the organization need to electronically access throughout the month in order to do their jobs. Two people are responsible for updating (writing) the information based upon a periodic analysis of other data, but the rest are only authorized to read specific subsets of the data fields contained in the view. Thousands of other people in the organization are not authorized to access this data view, but in many cases are authorized to access other data views in this same large database. How does the organization make the information available to the people that need it, while still denying access to everyone else?

Public key crypto technology may provide security for transporting this data, and authenticating the people who want to access it, but it does not solve the problem of differentiated access to data fields for those 208 people.

One way of solving the problem is to have a second database field containing the names (or other identity) of the people authorized to access each data field, along with a third field specifying whether each person has read, write, or read/write access. But this approach, if applied throughout the database, would make it impossibly large, and it doesn't work for non-database information that is kept on other servers (e.g., memos, reports, spreadsheets, pictures, etc.).

A variation on the above is to build a special security server called a *Permissions Server*, and keep access rights for all users in its security database. Thus, when a user requests information from a specific view of the data in the corporate database, the requestor is first sent to the permissions server, where he/she is authenticated and the view request is logged. The permissions server then checks the requestor's access rights in its own secure database, retrieves the information from the corporate repository and presents it to the user. However, the drawback to this approach is that the permission server is a single point of failure as well as a performance bottleneck, as all people accessing data must queue up to the permissions server and typically perform one or more public key authentication steps—each of which is a computationally intensive task that substantially reduces system throughput.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Another approach to solving this problem would be to encrypt each field and send all 208 people the appropriate symmetric encryption keys, and eliminate the permissions server. However, this solution will also grow to impossible key management proportions if applied to all of the millions of data fields and thousands of people who need access to them.

Still another approach—and the one currently in use at many government agencies—is to maintain multiple databases of portions of the same information, and allow classes of users to have password access to specific databases (e.g., an administrative database, an executive database, a scientific database, a legal database, etc.) This approach provides for data separation and very "large-grained" conditional access for a small number of functional groups, but is expensive to set up and maintain because of the excess duplication.

This need for "fine-grained" differentiated access is generic to large organizations and is not well solved by conventional PKI-based techniques. Traditional PKI systems have three major limitations:

- **Coarse-grained access.** Public key systems do not provide a good one-to-many solution to accessing parts of an information repository. If a member has the access rights to read a file, document or database view, he/she has the right to read *all* of it, and not just some of it. The ideal access control technology would allow different people to somehow view different parts of a single report, plan, database query, or financial spreadsheet, and deny them access to other parts. Traditional PKI cannot do this.
- **Centralized security adjudication.** Public key systems have a negative impact on computer system performance because of the computationally intense nature of public key exponentiation, coupled with the centralized nature of the security checking. When security servers or permissions servers are used to authenticate and police user information access, as the number of users and pieces of information in the system grow, they invariably become performance and single-point-of-failure bottlenecks—they simply do not scale gracefully.
- **No standardized credentials.** PKI systems do not comprehend the problem of providing credentials to people that would define their access rights to information. That is, a traditional PKI system can authenticate someone, but cannot easily solve the question of what information in the corporate repository that person is entitled to either create or access.

But now, TECSEC Inc. has invented a new distributed cryptographic key management technology that can efficiently solve the differentiated information access problem, and thus provide the final piece necessary to satisfy both industry and government with regard to electronic information access—and it is exportable with any crypto algorithm or key length. TECSEC has several patents on this technology, which is called CKM® for Constructive Key Management®, and is partnering with Ulogon.com, who will build a web-centric CKM security service ("WebCKM") that will be available to all customers on a monthly "rental" basis.

Currently, the United States Postal Service is evaluating CKM technology and a multi-year contract with TECSEC to provide a new CKM-enabled™ certified electronic mail system (internal code name of "NetPost.Certify") which will be used by millions of U.S. companies to transmit

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 24 of 115

mandatory governmental reports and other information to Federal agencies. Meanwhile, other large governmental agencies have discovered CKM technology, and are queuing up to use it for their own internal information access needs.

The purpose of this paper is to provide the reader with an overview of the CKM technology and its applications via a WebCKM security service from Ulogon.com. This paper defines concepts that are being developed and deployed in products from TECSEC and Ulogon.com. See www.tecsec.com and www.ulogon.com for more details concerning current product offerings.

The assumptions made in construction of this technology overview are:

- The reader has a fundamental understanding of asymmetric (public-key) and symmetric cryptography. If this is not true, send an email message to wbsweet@ulogon.com and he will send you an executive tutorial on cryptography that is easy to absorb and that will allow you to understand the underlying cryptography behind CKM.
- No inference should be drawn that TECSEC is representing CKM as having approvals by governmental or independent bodies other than those stated herein, including current approvals to key US Government classified information.
- This paper is a summary and significant details have not been included. Should a reader need to have a more detailed explanation regarding CKM or its potential for a specific application, please contact TECSEC Incorporated or Ulogon.com.

1.1 CKM Technology: A Fast Overview

CKM is a distributed cryptographic key management system consisting of one or more domains. Workgroup Administrators determine which members will be allowed to participate in each domain by issuing profiles to each member. Contained within each profile are each member's access rights that allow him or her to participate based on their role in the organization.

The key used to encrypt a data object in CKM is a symmetric key called the working key, typically a 3 key triple DES key. The CKM process employs three key values that are used to construct the working key: a Domain (key) value, a Maintenance (key) value, and a Random (key) value. In the most recent version of CKM—Version 5.0—the maintenance value can also be selectable as one of multiple different values.

The Domain value is used as a system key that gives system access to everyone in the domain. (In large organizations, domains can be linked together via trusted relationships, so no organization is too large for CKM technology.) Maintenance values are used to control domain membership by periodically updating the Domain value to all authorized members. This process enables Workgroup Administrators to eliminate undesirable members from future access to the system by simply updating the maintenance value to only currently authorized individuals. It also allows precise time frame control over access to data for archival researchers, since they can be given only the maintenance values for the time period(s) to which they are allowed access. This vastly simplifies the typical public key infrastructure problem of publishing and maintaining a certificate revocation list.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

The third value used to create a working key is the Random value. A new random value is automatically generated each time an object is encrypted, making the working key a one time key, unique to an object. The working key itself is not stored, but is created at the beginning and discarded after use. It is subsequently recreated when needed, but only by members with the appropriate credentials.

To segregate access to data among different groups of authorized members, the random value is further protected by encrypting it with other keys, called "credentials." Applying credentials to data to be CKM-encrypted defines the readership for each object. Only those with all the credential key pieces corresponding to all the credentials used in encrypting that object can decrypt the random value necessary to decrypt the object.

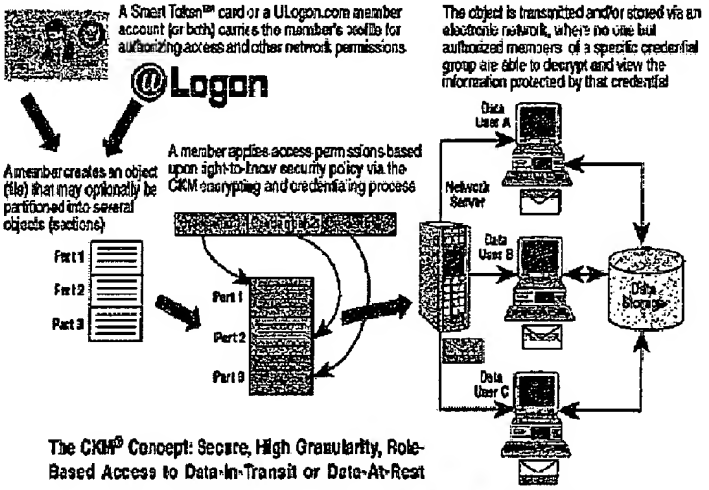
A member's profile, containing their credentials, the Domain and Maintenance values, the header encrypting key, algorithm access permissions, and domain-specific policies is contained in one of two places: either on a removable cryptographic token (e.g., a smart card), or on a central ULogon server profile maintained for each member and available over any Internet connection.)

CKM allows the distribution of encrypted objects to a broad audience where the distributor knows neither the identity nor the related access rights of each member of the audience. This provides the basis for the secure broadcast and storage of sensitive material over a network. New members to the audience are authorized according to their credentials as well.

In short, CKM allows organizations to do something they could not do before: make their repositories of critical information available to members over the Internet—securely and efficiently.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 26 of 115



The CKM® Concept: Secure, High Granularity, Role-Based Access to Data-In-Transit or Data-At-Rest

For example, sensitive corporate documents can be encrypted using CKM and placed on a company Intranet web server—without a centralized security or permissions server. Those employees with the appropriate access rights to individual documents may access each document (object), and each object may contain other objects within itself. Thus, users can access documents or parts of documents, and that access may be further constrained to read, write, or read/write permission. A single document or file may have as many objects within it as are required by the natural flow of the data within the organization.

Another example is a confidentiality-sensitive database containing medical information. Using CKM, a specific view of a selected set of fields—or subsets of the fields in that view—can be encrypted using differently credentialed random values. Doctors with one set of credentials could view a subset of a query report that contains relevant medical information, whereas administrative people could view the administrative information such as health care plan information, employer identity, etc. Administrators would be denied access to privacy-protected medical information such as a diagnosis (e.g., AIDS), and doctors would be denied access to financial information on patients they are not entitled to.

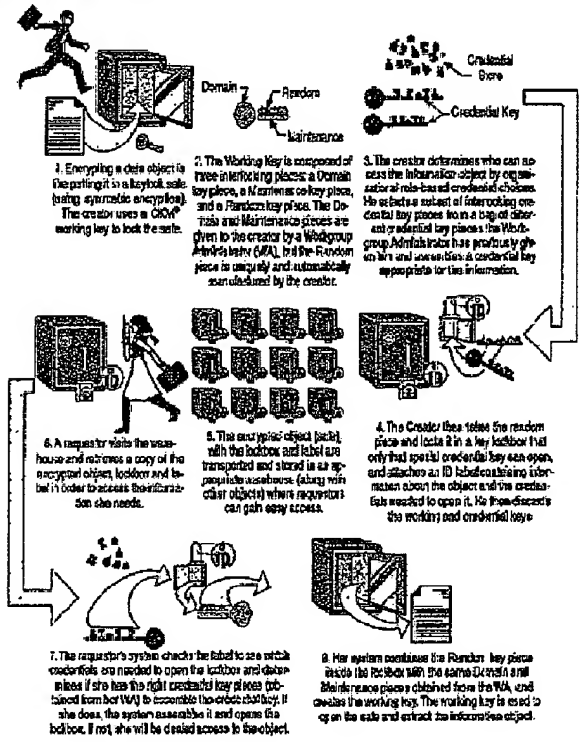
CKM is designed to be deployed as a secure system. This means employing two-factor security to protect the credentials, critical cryptographic protocols and private and secret encryption keys. With a smart card, the two factors are something you have (the card) and something you know (the PIN). With WebCKM, the two factors are something you are (a biometric authentication) and something you know (a PIN). Since a CKM system profiles are either protected by a secure smart card that can be removed and secured on the person when the member is away from his

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

computer, or kept inside a secure network server and available only via biometric authentication, (Ulogon.com), attackers have little capability to attack.

1.2 A Graphical Analogy

The following graphic illustrates an analogy to CKM that shows the roles of Domain, Maintenance and Random (key) values, as well as how credential keying materials are applied to construct and use the working key at both creation and access time.



A CKM analogy to locking up and accessing data objects

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

2. CKM Technology Details

Constructive Key Management (CKM) is a process by which an organization can manage the flow of and access to information at the basic object level. CKM is a cryptographic key management technique that embeds access attributes and other selected parameters within the object itself. The architecture is a flexible key management system that incorporates the strengths of both asymmetric and symmetric encryption elements, adding in the unique CKM techniques that bring the fine-grained role-based differential access. Included in the architecture is an encryption key generation process based on two sets of key types: working keys and credential keys. Working key values, credential key values, a combiner process to assemble these values and key components, and an infrastructure to support the distribution and management of the generated elements is what CKM technology is all about.

CKM is a key management architecture that is available in both symmetric and asymmetric models. The CKM trust model is based on a suite of financial community standards—the ANSI standards. The founding CKM standard is X9.69, "Framework for Key Management Extensions" for which the CKM design and infrastructure architecture is modeled. Key recovery is inherent in the design since CKM allows the System Owner 100% recovery of each encrypted object, and no third party key escrow is required.

The CKM key management architecture may be viewed as a whole system's identification, authentication, access control, and encryption cycle supported by a management infrastructure.

Some terminology is needed to understand the underlying process. The key used in the encryption of an object is called the *Working Key*. It may be used as a session key or a message-encrypting key that is required by a symmetric encryption algorithm such as 3DES. The working key, constructed from several pieces of information (called values), is used to initialize a symmetric key encryption algorithm, and is then discarded. The same pieces of information used in constructing the working key for encryption are used to reconstruct the working key for decryption. The function that combines the values to create a working key is called the *CKM Combiner* and is central to the CKM encrypting process. Member identifications, keying information and credentials are stored in a large file called a *Member Profile*, which typically travels with the member in a smart card or is accessible over the Internet in a central Ulogon.com server file.

Access control is provided in CKM by applying credentials in the encryption of keying information that is embedded in the object file header attached to the object. Asymmetric values are associated with each credential set. Read/write separation is cryptographically available with such an asymmetric key design. Read access is equivalent to decryption rights and write access is equivalent to encryption rights.

In addition to access control, a broader key management strategy may include a configurable identification capability and a third-party trust authentication capability as illustrated in the figure below.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 29 of 115

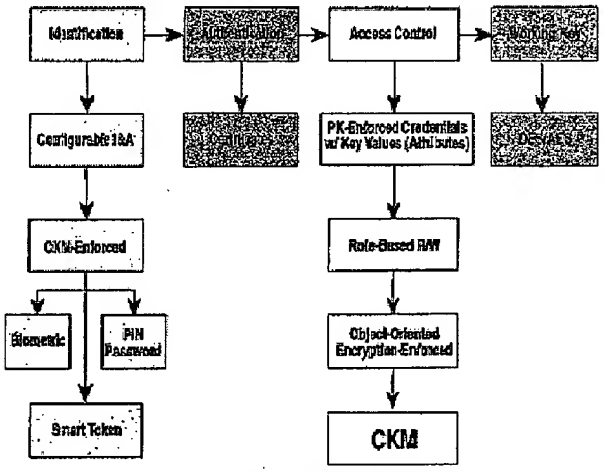


Figure 1: A flexible key management strategy

Credentials may be associated with an application that defines one or more member identity elements such as a biometric function, a smart card identity, or a PIN/Password. CKM is used to bind the identity elements to an encrypted object through an encryption process. The I&A (Identification & Authentication) object may consist of a Public Key Infrastructure (PKI) functions that can authenticate the member to the network and other members, and other functions that may need to be stored secretly and which are included in a Member Profile. The essential part of PKI is a certificate that includes a verifiable digital signature, which is itself a mathematical hash of information that is then encrypted through an asymmetric (public key) process. The PKI authentication support is managed through either the smart card or the central Ulogon.com server.

The figure below illustrates a Ulogon.com server and its interaction with a configurable Identification and Authentication (I&A) process;

1. Two types of asymmetric key pairs identified as Global and Membership;
2. Payment functions; and
3. Data that acts as a physical access function.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 30 of 115

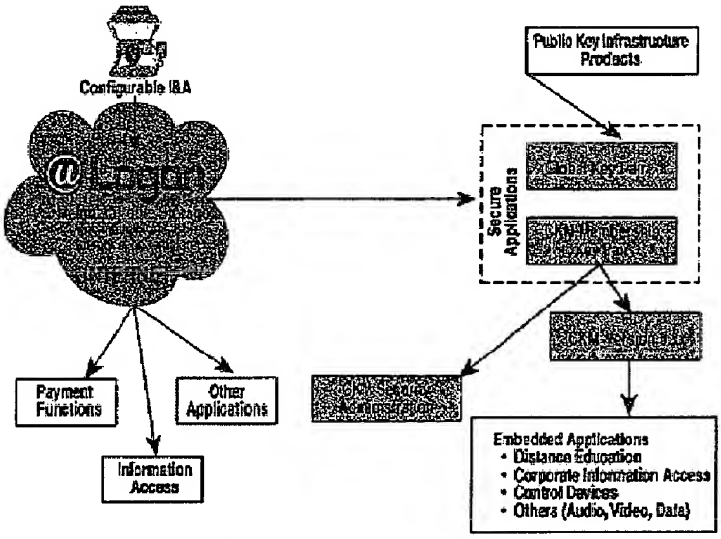


Figure 2: ULogon.com: avenue to comprehensive security

TheULogon.com Member Profile is used as a bridge to multiple authentication and encryption platforms with varying degrees of encryption enforcement and binding.

2.1 CKM Domain

Under a role-based access control system, rights and permissions are assigned to organizational roles, rather than to each member. As members' assignments change, their rights and permissions are changed to reflect their new roles. CKM, with its method of using credentials reflecting information flow and boundaries, is a preeminent example of a role-based system. The CKM design offers a method to anticipate data boundaries without knowing member identities.

CKM Administration is based on several core concepts that apply to any CKM setup—even if some are transparent. This section provides an introduction to each of these critical concepts.

The highest unit of organization in a CKM System is the *Domain*. A CKM Domain is a unique, independent entity that includes all CKM resources needed to function on its own. CKM security policies, procedures, and roles are all determined at the domain level.

Although it is the largest unit of organization supported within CKM, domains are fully scalable to a wide variety of needs. A CKM Domain may be as large as an entire enterprise or as small as a single member. One type of application might, for example, establish a unique domain for each

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 31 of 115

member, while small businesses would likely establish a single domain for the company, and large enterprises would establish many domains for major divisions, different locations, or other organizational structures.

While domains are freestanding and independent, they do not need to be isolated. CKM Domains may share access rights and privileges with other domains in a *trusted* relationship. Additionally, members may participate as members of multiple domains even if a trust relationship between the domains has not been established. The CKM Domain may have a direct relationship with a PKI Certificate Authority (CA), if so desired.

2.1.1 Trusted Domain Relationships

A CKM Domain may provide specified access rights and privileges to members of another domain by establishing a trust relationship. The trust relationship is established when one domain provides a subset of its CKM Credentials to another domain. Credentials are shared *only* at the domain level and may not be sent directly to members of another domain until a trusted relationship has been established. Once trust has been established, the second domain maintains and distributes "imported" credentials using its own methods and policies, and these credentials are stored in the same *Member Profile* as part of the member's credentials. Once distributed, members of the second domain may use the imported credentials to share information with members of the external domain, but they continue to be bound by the policies and procedures of the domain in which they hold membership—their *LogOn Domain*. If a PKI CA is included in the key management architecture, a third-party authentication model may be added to the overall trust relationship.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 32 of 115

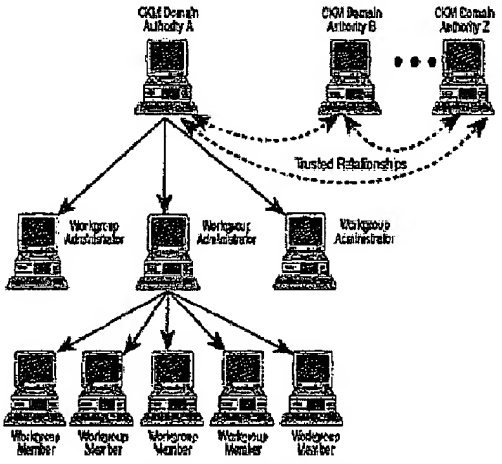


Figure 3: The CKM Hierarchy

2.1.2 Untrusted Domain Relationships

An individual may be a member of several CKM Domains regardless of whether the domains have established a trust relationship. That is, two or more domains may grant membership independently to the same individual. In this case, CKM sees the single individual as several members—one for each domain. In this type of untrusted relationship, the member will log onto each domain independently, use separate *Member Profiles* for each domain, and possess credentials only to access information within that domain (and with its trusted domains.)

Note: Some storage mediums (such as Smart Cards) currently do not have sufficient space to hold more than two or three Member Profiles. Therefore, the ability to log on to much more than two or three domains may require that additional cards be carried by the member. As time and semiconductor technology moves on, however, it is anticipated that smart card memory sizes (currently a maximum of 32KB) will increase substantially, thus providing room to carry a significantly larger number of Member Profiles. The WebCKM system, since it depends upon a central server to hold all profiles, does not have any practical limits on the number of profiles or the size of any corresponding data in each member's "connection profile."

2.1.3 Domain Authority

The Domain Authority (DA) provides top-level management to a CKM Domain. Although some decisions must be made by the person or persons assuming the responsibility of the Domain Authority, many DA functions may be automated.

Typically, the Domain Authority sets up the domain by performing the following functions:

- Names the domain and creates its unique *Domain Value* (used in cryptographic functions)
- Establishes and updates a number of *Maintenance Values* (used for revocation and to control information access to specific time windows)
- Sets policy defining the outer parameters of CKM use, including whether member Profiles are hard disk-resident, server-resident (WebCKM), or token-resident.
- Establishes and digitally signs the role-based *credentials* used by CKM to cryptographically enforce access control to information
- Selects and optionally renames the cryptographic algorithms available in the domain
- Selects and configures Identification & Authentication objects available in the domain
- Registers *workgroups* and their administrators through which credentials are distributed
- Digitally signs individual membership keys and authorizations related to CKM enrollment
- Registers and digitally signs CKM-enabled applications
- Creates and distributes *Workgroup Profiles* defining a subset of credentials, algorithm permissions and policy settings available to each workgroup
- Determines trust relationships with other domains

CKM allows members to receive credentials, policy settings, and algorithm permissions only if signed by the Domain Authority—even if some of these values are imported from other domains. Members are bound to the Domain Authority via the DA's CKM Membership Key and certificate issued to the member. The DA's CKM Membership Key is then used to verify the DA's signature when receiving credentials and related material.

2.1.4 Domain Profile

A Domain Profile refers to all credentials, policy settings, and algorithm permissions established by the Domain Authority and available within the domain. The Domain Profile also includes the domain's name and value, the maintenance value, and other information identifying the domain.

2.2 CKM Workgroups

A CKM Domain consists of at least one and usually several workgroups. A workgroup clusters members (or smaller workgroups) based on common needs and rights to information. Workgroups are often established to parallel departments, locations, projects, or other natural organizational subdivisions.

2.2.1 Workgroup Administrator

Workgroups are typically managed by a Workgroup Administrator (WA). The responsibilities performed at this level may be by a person interacting with software, or may be automated in part or in full. These responsibilities typically include the following:

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 34 of 115

- Refining policy settings (as allowed by the DA) to provide further restrictions than those originally granted to the Workgroup by the Domain Authority
- Registering the individuals who become the members of the Workgroup
- Assigning subsets of credentials and algorithm permissions available in the Workgroup Profile to individual *Member Profiles*
- Signing, distributing and updating *Member Profile Updates* to Workgroup Members

2.2.2 Workgroup Profile

The Workgroup Profile contains all credentials and algorithm permissions available for distribution to the members of a specific workgroup. It also includes the policies governing the workgroup's use of CKM. Workgroup Profiles may differ from other profiles in the same domain—defining the unique rights and needs of each group. Workgroup Profiles are created by the Domain Authority.

2.3 Member Profile

A *Member Profile* includes the credentials, algorithm permissions, and enforced policy settings assigned to an individual by a Workgroup Administrator. The Member Profile also includes the individual's private asymmetric CKM Membership Key used to decrypt profile and other membership information sent to the member by the Workgroup Administrator. The member's "public" CKM Membership Key is retained by the Workgroup Administrator and is not posted for public use as in a PKI. The Member Profile also includes the "public" CKM Membership Keys of the Domain Authority and Workgroup Administrator. Also, in WebCKM systems, it will also include one or more global and workgroup membership PKI (individual) private keys and digital certificates used for encryption or signing in WebCKM and other cryptographic systems. See Figure 2.

Members may receive profile and membership information from the single Workgroup Administrator whose Membership Key has been issued in the Member Profile. All updates to Member Profiles are signed by the Workgroup Administrator (WA) and must be verified by the WA's CKM Membership Key held by the member.

Members may be assigned to a different Workgroup Administrator only by receiving a new WA Membership Key signed by the Domain Authority. Additionally, credentials may be updated or added to the Member Profile only if signed by the Domain Authority and verified using the DA's CKM Membership Key held by the member. In this manner, each individual is bound to a specified workgroup and a specified domain.

2.3.1 Profile Storage

A Member Profile may take many forms. It may be stored locally on a member's workstation, on removable storage such as a floppy disk, on a network server such as Ulogon.com, or on a physical token such as a smart card. The form of the Member Profile is configurable by the DA. One of the policies carried within the profile determines where profiles are allowed to reside. The

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

form of the Member Profile is also dynamically scalable, i.e. if the profiles are not found in the one location, then CKM will look to the next location until the installed list of locations is exhausted. If a profile is not found in any of the allowed places, then CKM will prevent the member from initiating a session.

2.4. The CKM Process

2.4.1 The Security Paradigm and Data States

Adequate security is the condition at which protective measures have been employed that reduce the risk of loss to an acceptable operational and financial level. Total effectiveness depends on the synergistic interaction of various system features that reduce threats from inside and outside attackers and/or other vulnerabilities. This synergistic interaction forms a trust model. That is, one security measure alone does not provide adequate security. Only when all are taken together does adequate security result.

Encryption is a tool that mitigates certain vulnerabilities and thus reduces risk. To form an effective information security trust model, a member must be "bound" somehow to the data he or she is authorized to access. CKM technology begins with strong identification that is then directly bound to the encryption of objects via a credentialing process that in turn ensures the integrity and access control of the information being protected.

Since CKM is client-based, the trust model may be scaled to many members: 1) by distributing the workload to member workstations (desktops), and; 2) by making the encrypted object the basis of trust adjudication instead of a network-based server. *These are two critical differences between CKM and traditional PKI structures.* In a traditional PKI system, a front-end server protects access to the data, and the security focus is on authenticating each requesting member, both as to whom he/she is, and as to what information he/she may have access to. *With CKM, the typical PKI authentication step with a centralized security server is not required.* Once profiles have been distributed to members, encryption and decryption is controlled by individual member profiles, which typically will either reside on a smart card or a web server.

Data may be viewed at any given time of being in certain states:

1. Data at rest: data objects are in a fixed state in a storage capacity. An example of this state is a data field in a large centrally located database, or a series of documents resident on a network server.
2. Data in transit: data objects that are being transmitted in a communication channel during a period of time.
3. Data in process: data objects that are in static memory areas being manipulated by a computer operating system and/or one or more applications.

CKM can provide a key management and control scheme for both data-at-rest and data-in-transit. Data-in-process security is dependent for the most part on operating system and hardware-based control mechanisms.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 36 of 115

2.4.2 The CKM Combiner Function

The role of the CKM combiner is to create a working key from the domain, maintenance, and random values. The working key encryption process uses a standardized triple DES (3DES) algorithm. The output of the combiner function is the (3DES) working key as shown below.

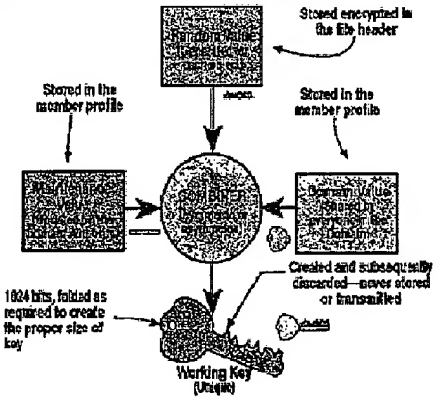


Figure 4: The CKM Combiner Function

The working key is destroyed immediately after an object is encrypted. In order for recipients to be able to decrypt the object, certain information is given to them either within an object header or via the member profile. The random value is encrypted with a key generated (assembled) by the credentials the encryptor (creator) selects. It is important to note that it is not possible to recreate the working key solely from information provided in the object header.

The working key is used with a symmetric encryption algorithm such as 3DES or a future U.S. Advanced Encryption Algorithm to encrypt the actual data object. Since the working key is destroyed immediately after an object is encrypted, information pointing to the specific data required (which a member may or may not have in his/her profile) to reconstruct and apply the values, credentials, and other functions are included in an encrypted header that anyone in the domain can open. The header-encrypting key is managed through the same distribution scheme as the maintenance value and credentials (e.g., distributed from a Workgroup Administrator's account at the Ulogon.com server to individual workgroup members' accounts at the same server), and all can be updated concurrently.

Read and write access, and the protection of the random value are accomplished through a combination Diffie-Hellman (asymmetric) process that creates random value encryption keys. Normally, symmetric key cryptography (3DES) is used for random value encryption. In the asymmetric credentialing process, a Diffie-Hellman static key pair is associated with each credential (piece) and the "public" key of each pair is used to derive keys that are then combined mathe-

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 37 of 115

matically to create sufficient keying material to encrypt the random value. A member with an appropriate set of Diffie-Hellman "public key"-based credentials may encrypt objects, and a member with the corresponding set of Diffie-Hellman "private key"-based credentials can decrypt those objects. A member with both sets has both read and write access. This process results in other parameters that are also included in the member's profile, and an additional level of assurance within the combiner functionality.

2.4.3 The CKM Header

A CKM object header must be available to decrypt an encrypted object. The CKM header contains, among other things, the encrypted random value used in constructing the working key. Since the header is encrypted with a header key known to all in the domain, the header of every object encrypted by CKM may be read by anyone in a workgroup belonging to the domain. Note that the random value is not available to those without cryptographic read permissions for *all* the credentials originally used in that specific object encryption process.

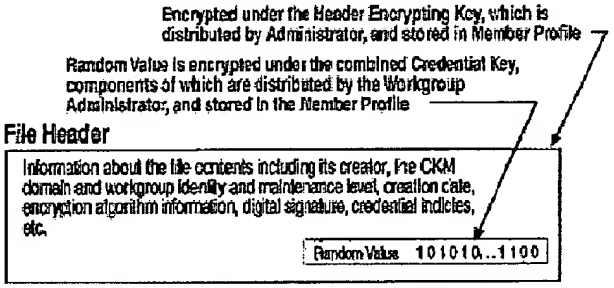


Figure 5. The File Header contains information about the file, along with the Random Value, which may optionally be encrypted with the combined credential key. The header is encrypted with the Header Encrypting Key, which all members of the domain possess.

2.4.4 The CKM Object Encryption Process

With CKM, a file or document may be encrypted with a working key. Alternatively, a component of that file or document (called an *Object*) may also be encrypted inside the main file with a working key different from the main file. With traditional PKI security methods, data objects can typically be no smaller than an individual file or database view. With CKM, however, an object can be as small as a single word within a file, or a data field within a database view (query, or report). This object-within-an-object architecture places no constraints on an organization's ability to apply CKM technology to its natural information segmentation—either when the data is at rest in a network-connected information repository, or while it is being transported across the network by several transport mechanisms (each providing a secure CKM "object wrapper" around the object being transported).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 38 of 115

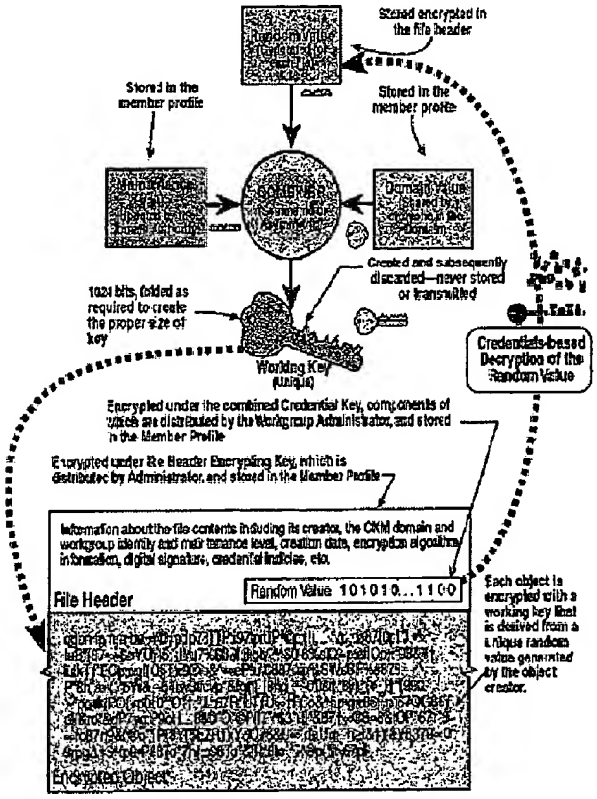


Figure 6. The detailed CKM process for a single object

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

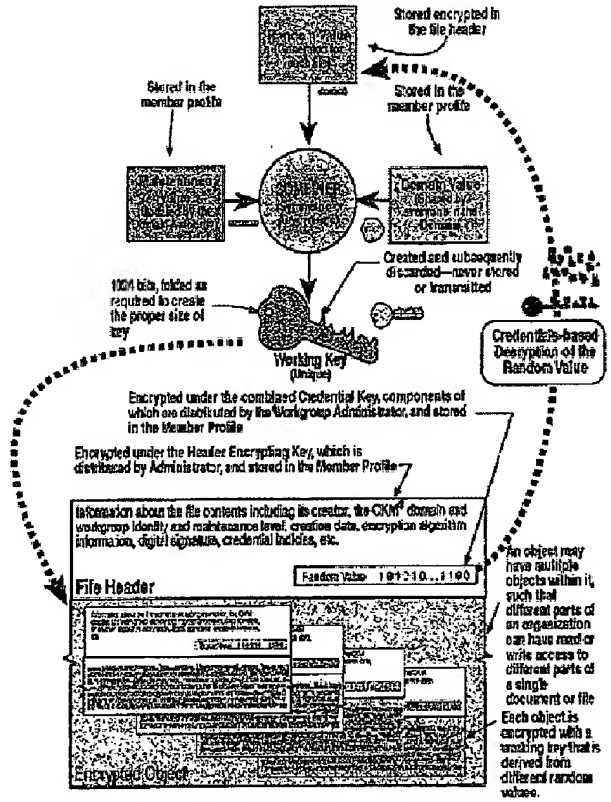


Figure 7. The detailed CKM process for multiple objects

With CKM, objects can be contained within objects. This is convenient for several reasons:

- When different people need to be granted different access rights to data objects within a document or database, each unique data group (e.g., sections within a business plan) can be designated as an object and included within a higher level object (the business plan.) In this case, lower level objects may be arranged within a higher level object in a parallel fashion.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 40 of 115

- When different transport mechanisms are used to move a data object, each may wrap the object it receives with its own CKM credentials (e.g., a local police department message, encrypted under that department's domain, then wrapped by the FBI domain on the Internet, and traveling over a State Department network, which applies a State Department CKM credentialing and encrypting process.)
- Alternatively, data objects may be organized in both hierarchical and parallel subdivisions, each architecture tracking the way in which an organization performs its mission. CKM can easily adapt its object hierarchy to fit almost any organization.

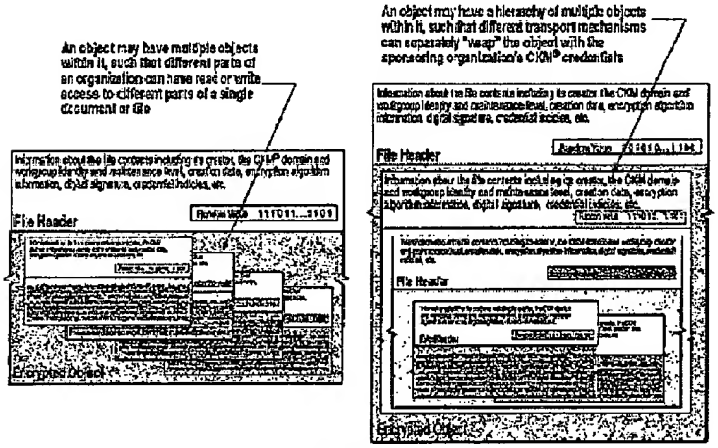


Figure 8: CKM object combinations

2.4.5 The CKM Credentialing Process

CKM is superior to other cryptosystems for many reasons, but the most important is that it allows differentiated role-based access to large databases of information. This process is initiated at the time the data is entered into the system. For example, in a large reporting document (file) with many sections, each section, chapter, paragraph (or word) can be credentialed and encrypted differently from the others, according to the roles selected for read or read/write access. A simple example of credentialing choices for the creator is shown below.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

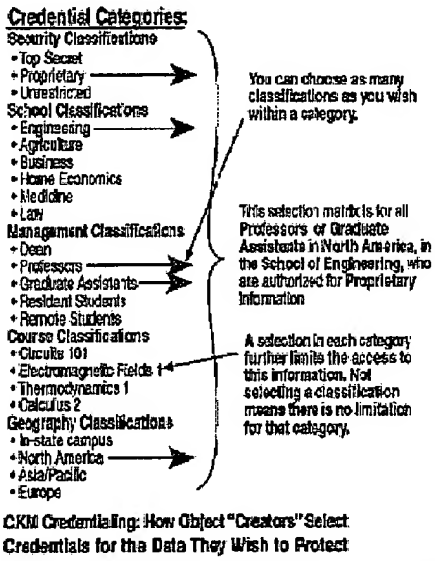


Figure 9. A simplified example of the CKM credentialing process in an educational setting

Credential categories and classifications are defined by the Domain Authority. Note that within the set of credential choices, multiple classifications selected within a category are ORed, while all Category choices are ANDed together conceptually to derive the credential keys used to encrypt the random value (e.g. [Proprietary] AND [Engineering] AND [Professors OR Graduate Assistants] AND [North America]). *All* credential categories included at the creation of the information must be available in the member profile of anyone wishing to access that information. If only one required credential category is missing, the object will be unavailable.

This CKM credentialing function brings two critical benefits to the access control problem:

- Credentials allow role-based access designations to be applied directly to a data object such that access can be controlled by the credentials held in a member's profile, thus eliminating the need for a permissions or security server;
- By providing a standardized way of creating and applying credentials that information creators can be trained to use consistently throughout a domain, CKM brings a new standard methodology that substantially enhances information access for organizations of all kinds.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 42 of 115

2.4.6 The CKM Session

The Domain Authority sets, and Workgroup Administrators enforce session timeouts for members. Based on the security risk, the maximum idle time during each CKM session may be centrally controlled. Session timeouts are included in each member's profile and may not be reset by the member. Generally, the member is required to repeat the identification and authentication process in order to restart a timed-out session.

2.4.7 Identification and Authentication

Identification is the process of identifying the member. Authentication is the process of validating that identity. CKM profiles are encrypted with an identity process. In order to access profiles, members must provide proof of identity. This proof may consist of presenting valid User Identification (UID) along with a correct password (PIN). It may also consist of presenting a biometric scan such as facial contours, voice recognition, or lip movement while speaking a passphrase. Authentication occurs at the workstation when valid identification is presented for the profile that was issued by a Workgroup Administrator.

A Workgroup Administrator creates each member's profile. Among the data included in each profile is the member's identification. The member may not change the UID supplied by the Workgroup Administrator. Each time an object is encrypted, the identity of the profile used is placed in the header so each recipient may verify the identity of the encryptor. Trust is assumed since only a Workgroup Administrator may issue profiles and only a Workgroup Administrator may designate UIDs.

2.4.8 Revocation of Member Access

Any cryptosystem must have the means to revoke a member's access. Revocation refers to preventing access to material encrypted subsequent to revocation. It does not refer to preventing access to material encrypted during a member's period of legitimate access. Once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant. CKM has multiple means to revoke members. The basic CKM revocation methods are listed below:

- Profile expiration limits provide a routine, periodic method of removing member access, just as credit cards expire. As profiles expire, they may simply not be renewed.
- Updated maintenance values eliminate access to those without the new value. New maintenance values have backward utility so that material encrypted with a previous maintenance value may be decrypted with a subsequently issued one. The DA may choose to issue a new maintenance value and not give it to certain members, thus revoking their access to future information. Periodically, new maintenance root values may be issued that do not have backward utility, thus marking the beginning of a new time period. Multiple maintenance values and multiple roots allow fine-grained control over time periods.
- Maintenance values can be used as "time release" factors for time sensitive materials. For example, course materials may be issued to a student by an educational institution, and

new maintenance values may be issued at the beginning of each week to "unlock" content appropriate for that week's study or testing.

- An advantage of a web-centric CKM system (Ulogon.com) is that member profiles can be cancelled or changed any time with virtually immediate effect. As members connect to the central site to use their member profiles to access old content or create new content, their credentials can be changed from the last access. This facility is particularly useful in responding to—or preventing—certain security attacks by outsiders and/or former workgroup members, since all an administrator has to do to forestall such attacks is cancel a rogue member's credentials. This is a more difficult problem for smart card-based systems, since a rogue member could continue accessing content up until the credentials on the card finally time out.

2.4.9 Key Recovery

Key recovery refers to the ability to recreate or retrieve working keys. CKM technology is unique in that unlike in private key escrow and session key escrow, CKM does not escrow anything. CKM provides the Domain Authority—and to a limited extent the Workgroup Administrator—with the ability to reconstruct all working keys, since the DA created all the system keys, as well as all the credentials. If the header or its equivalent is made available to the DA, the working key can be reconstructed.

This key recoverability of CKM is a critical advantage for two reasons:

First, all organizations need an ability to recover encrypted files when the primary encryption keys have been lost. Modern high strength encryption is virtually unbreakable; so locking up vital intellectual property and then losing the keys means that data would be lost forever. In typical commercial use, employee turnover, computer failures, loss of tokens, and other catastrophes happen to a significant percentage of organizations every year. Thus, it is in the organization's best financial and security interests to have a simple recovery capability in case a workgroup member loses his or her keys. CKM provides a simple key recovery capability.

Second, modern high strength symmetric encryption is subject to government control in many countries. In the United States, the export of strong encryption is regulated. These regulations are continually being revised to address the demands of electronic commerce and national security issues. TECSEC has been granted a unique export license for CKM technology. See Appendix B for more details.

2.4.10 A Word About Databases...

CKM usage with normal electronic document files is fairly straightforward. Data objects are encrypted with specific CKM working keys, grouped into object hierarchies and stored on network-available magnetic or optical storage devices for access by a multitude of members with the appropriate credentials.

Databases, however, are another problem. Because large relational databases need to conduct internal operations on the data contained within, encrypting each field can pose a problem. How can a database sort data, calculate indexes, create calculated values (from multiple data fields),

and perform ad hoc inquiries if each field is encrypted? If encrypted with CKM, how would the database know what working keys to use? Where would such information be stored? This is a case where encrypting the data for security reasons may get in the way of managing that data within a relational database.

A number of techniques have been developed to solve this problem as follows:

- Members filling out database forms for submission to the database do not necessarily need to worry about which credentials are to be applied to each field. Special templates are created which present preformatted electronic input forms for members to key in the data. Each template carries within it the index values of the preset credentials associated with each data field. Thus, clerical staff need not even know what credentials are being applied—all they know is the data is entered and sent on its way when completed, using their member profiles and their desktop systems to perform the necessary encrypting and digital signing of objects.
- CKM-encrypted data may be stored directly within the database structure. If it is done this way, database indexing must be simple (e.g., based on serial numbers) and file header information must also be kept in order for the database to decrypt data fields for internal maintenance purposes. This provides for substantial protection against hackers that might search the magnetic or optical media with analytical tools. However, it makes ad hoc searches of the data difficult to conduct.
- One approach is to decrypt all data coming into the database and store it within the database structure as plain text (non-encrypted). Since all members depositing or viewing data must do so through predetermined views of the data that are controlled, formatted and presented by view templates running on a DBMS query processor, it is a simple matter to include CKM encrypting and decrypting operations as a part of the database templating process. Thus, when a member requests a specific view of the data, the database references the template selected, reads the credentialing information for each field, fetches the data and encrypts it with the appropriate working key, storing the encrypted Random value within the object header in the normal fashion. The member then retrieves the CKM-encrypted data and uses his/her member profile to access that data for whatever job task is under way.
- A variation on the above approach is to use a single secret symmetric key to encrypt all the data in the database, thus providing protection against hackers that might search the storage medium with sophisticated analytical tools. This inserts a decryption/encryption step into all database access for either internal or external use, but nevertheless is perfectly workable. All CKM credentialing and encrypting operations are still handled by the templating process.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 45 of 115

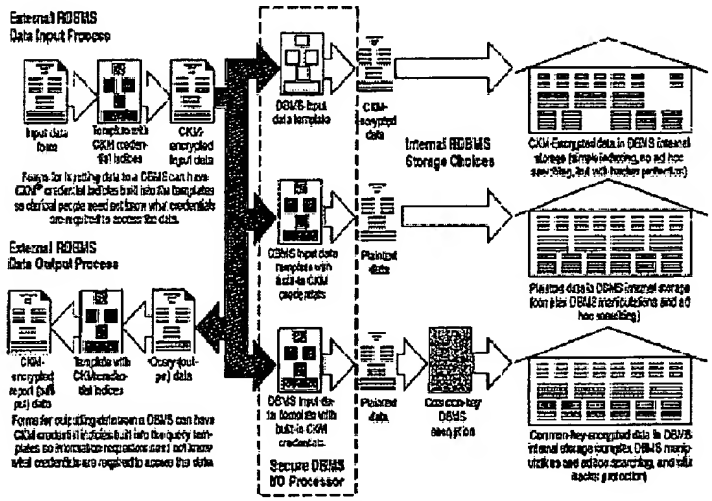


Figure 10. CKM database security choices

Since different organizations have different security policies pertaining to the architecture and management of their databases, there are a number of solutions—and combinations of solutions—available to deal with the database maintenance problem. A number of large Federal agencies are currently working with the major database and template companies to perfect the most optimum ways of storing and retrieving CKM-enabled data to and from Federal databases. Undoubtedly newer and better variations will continue to evolve as these organizations gain more experience in deploying CKM-enabled systems.

A major advantage of CKM is that many people with different data access rights may all request and obtain the same standard database input or query form over the network. Since different data fields may have different credentials applied to them, only the information appropriate to each member is made available to that member. This allows a single database system to serve the needs of potentially thousands of people, each inputting or outputting only data related to their job roles, but with all members sharing a standard set of templated forms and the same (non-duplicated) data repository.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 46 of 115

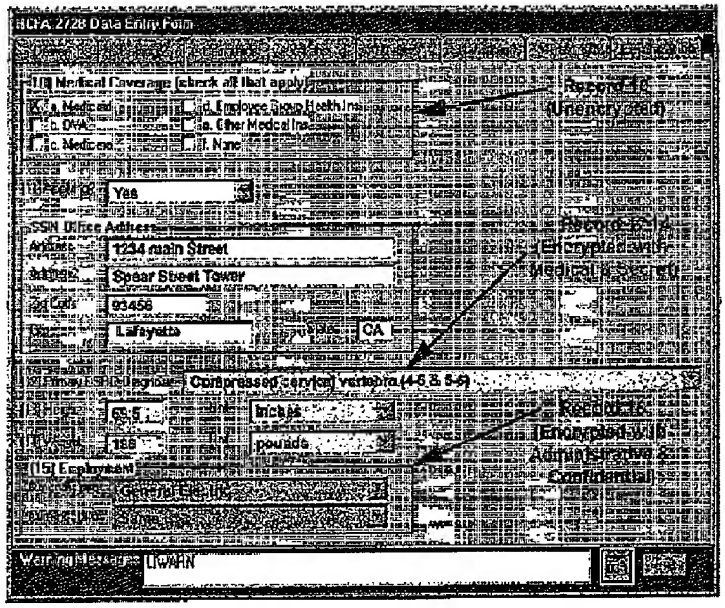


Figure 11. An example of a database query form encrypted with multiple credential sets.

4. Member Profile Storage Choices

4.1 The Smart Card—A Decentralized Profile Storage Scheme

A smart card is a thin piece of plastic the size of a credit card but with a processor, read/write memory, and metal contacts so that Input/Output (I/O) can take place. ISO 7816 provides the specification for smart cards. A CKM-enabled Smart Token card stores Member Profiles. I/O between an ISO smart card and a workstation can be relatively slow, making session logon relatively lengthy. Nevertheless, with the greater storage and processing capability becoming available today, smart cards hold much promise for secure, portable information storage, as well as possessing the advantage of three-factor security (something you know (a PIN), plus something you have (the smart card), plus something you are (biometrics)).

Secure storage in the case of a Smart Token card means that data is either stored in a secure area of memory that can only be accessed by the smart card operating system, or data is encrypted with keys stored in a secure area of memory.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

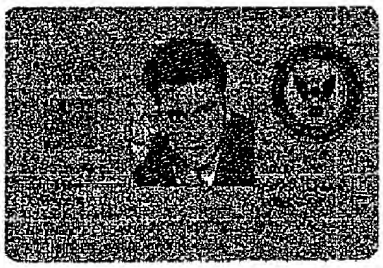


Figure 12: An example of a Smart Token card

Smart cards are a secure and portable CKM profile storage option. They hold a member's profile information and the critical encryption algorithms, and are removed from the system (card reader) and secured on the person when the member does not wish to be on-line. This makes it extremely difficult for attackers to hack into the security system since:

- Credentials (member profile) and critical crypto algorithms such as sign and verify and key assembly (combiner) are *not* on the workstation or the workstation's hard drive, but on a secure Smart Token card.
- The network has no access to the smart card in the card reader, and if a smart card is found by an attacker, it will not function without the member's PIN and/or biometric scan data.
- The card allows for portability and flexibility. A member may move from one computing or access device to another and still have appropriate access.

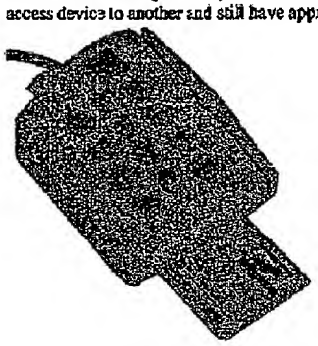


Figure 13. An example of a smart card reader with integral PIN pad.

CrypTEC Systems and TECSEC Incorporated are currently developing a secure smart card with enhanced storage and processing, as well as hardware random number generation capability.

asymmetric key pair generation, and tamper detection. This smart card is called the Smart Token card. It currently uses a smart card micro-controller with 32KB of EEPROM memory, 32KB of ROM memory, and an attached crypto coprocessor. It will eventually use up to a 32-bit processor and carry several megabytes of storage. The crypto coprocessor performs large number math and bit manipulation very rapidly, substantially improving the processing speed of cryptographic algorithms. Certain areas of memory will only be readable by the card operating system, thus protecting keying material. Since Member Profiles and the CKM processes that create working keys will reside on the card, only session logon information and working keys for large objects need to be exchanged via card I/O. Larger profile files need to be communicated across the card I/O only during profile installation and activation, so the smart card bandwidth limitations are not a system performance factor.

Another feature being developed is the inclusion of a biometric capability. This capability with a smart card would allow a high level of security with strong UID, as well as the ability to store different types of information about the member in a package that is easy to carry and easy to use. At present, several fingerprint devices are available on the market, as well as facial recognition, speech recognition, and lip movement recognition devices.

4.2 The Ulogon .com Web Service—A Centralized Member Profile Scheme

An alternative to the approach of utilizing smart cards and readers at each desktop to contain a member's profile is to place that profile on a secure web server, and access it when needed via the Internet. With this approach, the smart card and reader may be eliminated from the system, and CKM functionality can essentially be rented on a month-by-month or week-by-week basis.

The ULogon model essentially moves the smart card functions to a secure ULogon server, using a profile unique to the user and the domain(s) he/she belongs to. The desktop still would encrypt and decrypt files, and would rely upon the ULogon server for signing and verifying and all working key creation. The server would hold all private keys and certificates, the user's CKM profile, including credentials, and the Biometric templates. The server will have a "member profile" for each user and administrators will simply transmit credentials and other periodic maintenance details to users via their server-based mailbox instead of via email. Domain and Workgroup Administrators will perform their administrative chores via connection to the ULogon web site, instead of on their local systems.

Since the wire connecting the ULogon server-based user profile (containing the equivalent of the smart card) is now quite long (the Internet) and vulnerable to attack, Diffie-Hellman key exchange routines are used by both the server and the desktop, so the desktop and server can exchange private information securely, such as working keys, command requests, message digests to be signed, etc. This means that a user will need to have a reliable connection to the ULogon server, since every time an object needs signing or verifying, or every time a working key needs to be constructed to create or access an encrypted object, the server will have to be engaged. This also means that if the server or the network goes down, the user is temporarily out of work.

However, there are some advantages to the centralized ULogon approach, including:

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

1. Lower costs of entry for the customer; instead of paying, say $50–$100/seat for the CKM software license and $50/seat for a CDROM, smart card and reader, the user can now pay a smaller monthly rate, say, $8-10/seat/month

2. Mobility; A user can now travel the web and log in from anywhere. (He may need to drag a video camera and microphone and a CD around with him if he uses BioID, which uses facial, voice and lip movement as biometric authentication modes.)

3. Convenience; the big expense in deploying CKM is not the cost per seat or the card and reader, but rather the training and systems integration work necessary to setting up the infrastructure—especially training Domain Authorities and Workgroup Administrators. Thus, a central web-based approach can provide a lot of convenience, including:

- A professional and readily accessible training tool (access the site for training programs)
- An easy way to download necessary user and administrative software modules
- An easy way to set up and maintain domain and workgroup administrative functions
- No smart card hardware to install or debug
- Larger and more numerous domains and biometric templates can be managed (no smart card memory constraints)
- Using BioID, member enrollment will be much easier since it can be carried out on-line via a video/audio/keyboard chat interview using the BioID for authentication. Enrollees can even hold their passports or drivers licenses up to the camera.
- Guest users and pilot tests can be created overnight
- The bureaucratic hassle associated with setting up a new (CKM-based) security access control system within a large company can be avoided, since the web-hosted CKM service is "self-contained," easy to acquire and use, and can be purchased by lower management budget authority.

4. Better security

- Using BioID, users can be authenticated better (use both BioID and passwords for better security), since passwords are easier to defeat and users can give them to each other if they wish
- WebCKM has substantially less potential for illegal surreptitious access to administrative systems during off hours, better authentication of the administrator, and much reduced requirements for physical security.
- WebCKM has rapid response to maintaining users and foiling security attacks (can change anyone's status immediately and thus reduce the risk of rogue users)

The Centralized Smart Card Model

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

A variation on the centralized server model is to use smart cards or other tokens at each desktop, and yet require each user to log in to a central server once a day to be synchronized with the centrally-maintained credentials files and to utilize the BioID authentication to the smart card. If a user has additional needs for Ulogon's Virtual Presence or Virtual Interactivity services, then logging in every day will become a normal part of the work schedule.

5. The Power of CKM: Solutions

Cryptography and its related elements are generally viewed as merely a utility, the sole purpose of which is to provide security and confidentiality to data and voice storage and communications. This is true of most cryptographic key management schemes and encryption software applications. However, it is not true for CKM. The ability to selectively encrypt objects within objects and the granting of role-based access to these objects sets CKM apart from other key management methods. CKM attributes provide the basis for solving business communications problems in uniquely beneficial ways.

One-to-Many Distribution

CKM allows for a one-to-many distribution of encrypted objects where the creator does not know the identity and related access rights of the many, including future members within the domain. This provides the basis for secure broadcast of sensitive material. Secure CKM one-to-many distributions can be used for numerous corporate, employee, medical, customer, and vendor applications.

Dynamic Data Separation

CKM separates data cryptographically. Each set of credentials used within a domain separate that data from all other data within the domain. This data separation is enforced cryptographically, and not by separate physical architectures. With CKM, data separation—including layers within layers (objects within objects)—can be dynamically changed to meet organizational requirements regarding information flow and access boundaries. In essence, CKM can provide dynamic, cryptographically enforced private networks within a larger organizational network.

Distinct Separate Reality

CKM can take one or more encrypted objects and encrypt them within another encrypted object. It is this object-within-an-object that provides CKM with the ability to selectively decrypt objects according to access rights previously given to members.

For example, management desires to post a memorandum to all employees on its Intranet web server. In addition, management wishes to include additional confidential information for Managers. With CKM, the portion of the document intended for all employees would be encrypted with credentials every member in the domain possesses. The portion of the document pertaining to management would be encrypted using a credential limited to managers. When employees download and decrypt the document, all employees would view the common information. Managers would also view the restricted information. With CKM, it is possible to have each member view an object or objects and not know their access differs from others.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 51 of 115

Flexible Role and Responsibility Assignment

CKM and the Smart Token do not exist in a vacuum. Other parts of the system reside on the member's desktop computer, and on the administrator's computer system elsewhere on the network. Servers are not required by the CKM architecture, but the architecture will accommodate servers easily in the system if required.

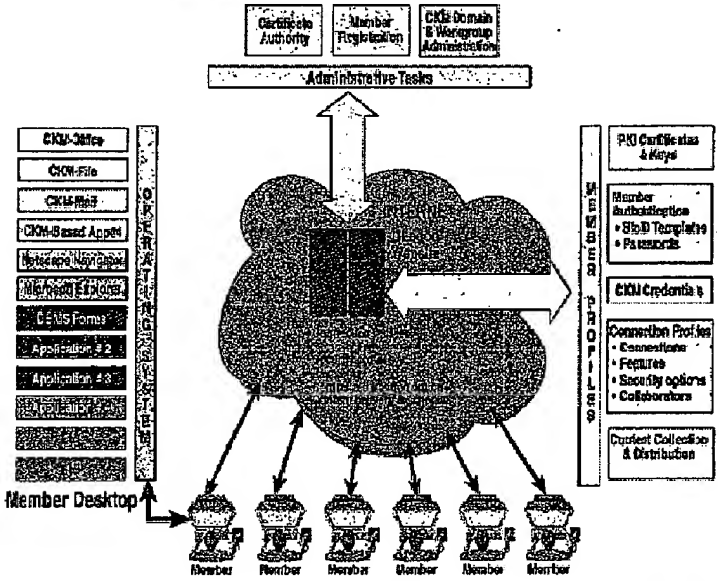


Figure 17. The CKM security layer for a typical web-based system is shown above. It consists of the CKM modules located on the member's personal computer, as well as connections through the Internet to the Ulogon web site for access to the member's keys, certificates and member profile. Another critical set of functions resides on the Ulogon server for the Workgroup Administrator and Domain Authority.

Administrative functions may be separated into as many levels as needed for security and workload needs. Organizations may continue to use the included 3-tier system consisting of a Domain Authority, Workgroup Administrators and Workgroup Members, or they may customize this system for more or less separation of functions and levels of distribution.

Administrative roles and responsibilities are not bound, a priori, to any level or component. If the standard role assignments of Domain Authority, Workgroup Administrator, and Workgroup

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Member do not meet an organization's needs, applications may be customized for other assignments. Responsibilities may be moved up or down the distribution hierarchy, or roles may be assigned in a completely different manner.

5.1 The U.S. Postal System and certified electronic mail

The U.S. Government, through several Congressional Acts, has mandated that all required document submissions to all federal agencies must be electronic by March 2003. The anticipated savings to both governments and companies are astronomical, and run into the hundreds of billions of dollars per year. However, just getting the information to the government securely is only part of the problem. The most important part is making that data securely and efficiently available to the people who must access it throughout industry and government.

The United States Postal Service is evaluating a new secure certified electronic mail system for industry and government that will enable the submission of these documents electronically in place of the centuries-old paper method. This system has been called "eProof" internally, but will most likely have the new name of "NetPost.Certify" for formal introduction (anticipated in Summer of 2000).

Through this new certified email service, a corporation sending mandatory data to a Federal agency would do so through the Internet and a USPS smart card. A corporate member would typically possess two sets of credentials---one for the USPS transport process over the Internet, and one corresponding to the domain of the Federal agency the data is being sent to. The data would be broken into objects, each encrypted with a working key protected by a specific set of credentials associated with the agency's domain. If required by the agency, all objects in a particular submission could be "wrapped" (encrypted) again using a broader level of credentials such that only members of that domain could open the complete data package (some of which may have been designated as unencrypted). The encrypted package would then be wrapped again (encrypted) with a set of working keys and credentials associated with the USPS, and the multiply-encrypted package would be sent to the Federal Agency.

Upon receipt of the data package, the agency would "open" (decrypt) the USPS wrapper, send notification of receipt to a USPS server, which would return a date and time-stamped certified notice to both the agency and the submitting corporation (the certified email receipt). Upon receipt of the USPS certification, the agency would open its domain wrapper and send the encrypted objects to wherever they need to reside within the agency for further processing and storage (typically a database management system).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 53 of 115

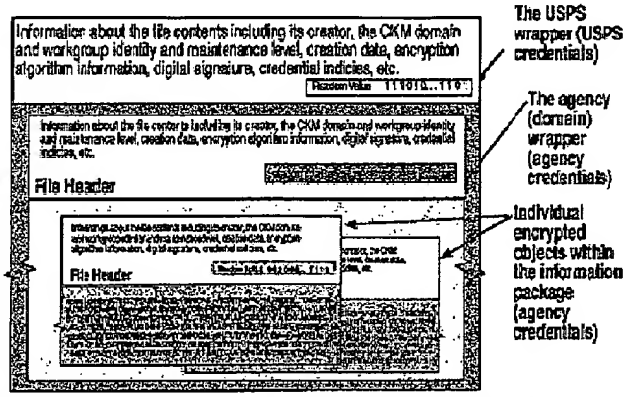


Figure 18. The proposed USPS object hierarchy for a typical data submission to a Federal agency.

All of these data transmissions can take place over the Internet as pieces of electronic mail—quickly, inexpensively, and securely.

The USPS plans to charge less than typical paper-based certified mail for each such transmission. The target markets are business-to-government, state-to-federal-government, and business-to-business. The first major customers for the service are anticipated to be the IRS, the Social Security Administration and the Health Care Financing Administration, which processes Medicare/Medicaid data on behalf of 75 million Americans.

The USPS—the only commercial entity in the US that can issue electronic credentials for e-commerce for which the penalty for tampering is a federal felony—would provide and maintain the infrastructure for certified email usage, principally consisting of the readers and smart cards and desktop software for members, as well as the administrative CKM functionality for government agencies and corporations. The USPS would also provide the certificate authority for issuing certificates to members, as well as the smart card initialization and personalization functions necessary for registering new members and issuing cards to them.

CKM is the necessary USPS technology that provides the secure fine-grained differentiated access to authorized information users within the government and corporate worlds. Smart cards with CKM-enabled functionality are essential to this service. Currently, the USPS is negotiating a multi-year contract with TECSEC to design and implement the new secure electronic USPS system using CKM technology.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 54 of 115

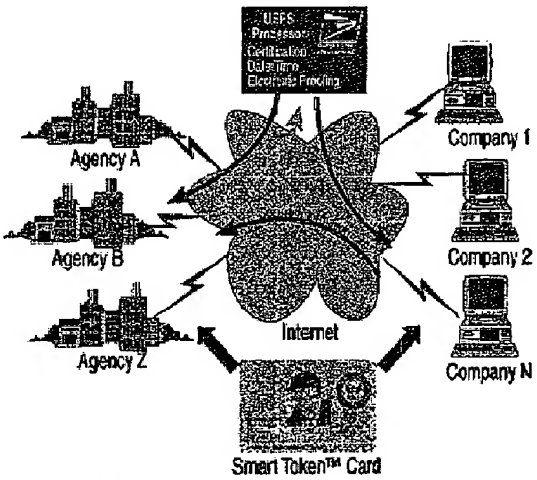


Figure The USPS certified email system would deliver secure certified email to government agencies and return a receipt of delivery.

Other government agencies are also evaluating the "NetPost.Certify" system over time for their document submissions from the commercial world.

Once the industry-to-government and government-to-government document transfer system is up and running, the USPS could take this service to the world as a company-to-company service, and ultimately as a consumer-to-consumer service. Other post office agencies in many countries are already interested in adopting this technology, and many may follow the USPS's lead and offer similar or identical services in their countries. Since CKM crypto is exportable around the world, there should be no legal or national security issues involved in rapidly expanding USPS/CKM technology to the rest of the world. Obviously, adoption of this CKM-enabled technology by the world's post offices would establish CKM as a de facto as well as official standard for secure, exportable, certified access to information.

6. Conclusion

CKM is a powerful key management technology that has substantial advantages over other more conventional key management systems. CKM is flexible and may exist with and use the strong attributes of public key infrastructures, such as identification and authentication, to form a superior combined key management and encryption system.

CKM brings substantial advantages to organizations, including:

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

- Distributed role-based access control: CKM's distributed role-based access control, one-to-many distribution and data separation characteristics allow organizations to tailor their crypto security to suit the way their information is created, distributed, consumed and stored—a much better solution than the centralized, one-to-one nature of traditional public key cryptosystems.
- Fine-grained access: CKM allows documents and files to be split up into separate objects, and objects may have other objects within them. This capability allows different parts of a document or file to each require different credentials for access, and thus allows organizations to precisely map information access to the way in which the information naturally flows within the day-to-day workflow.
- Key recovery: CKM's architecture makes it possible for Domain Authorities to provide access to encrypted files for which the key values have been lost by members. This has two benefits: (1) organizations can encrypt their critical information without fear of loss due to lost keys; and (2) CKM satisfies the emergency access needs of criminal investigation and national security authorities (a court order can compel a workgroup administrator to recreate the necessary keys), and is thus easily exportable around the world.
- Versatility: CKM is extremely flexible, and is compatible with traditional public key infrastructures, and can be implemented with smart cards to hold member profiles, or with a WebCKM server (Ulogon.com). Alternatively, CKM can be used without a PKI, and still remain flexible and scalable.
- Industry standard: CKM is an ANSI X9.69 standard, and may soon be deployed by the US Postal Service for a new secure certified electronic mail system that will be used by government and industry to enable true paperless communications. Since postal systems must be compatible around the world, other nations may also be adopting CKM-based electronic postal services. This would make CKM a worldwide de facto standard that will insure its presence for some time to come.
- Performance and Scalability: Public key crypto has a debilitating effect on a computer performance, and centralized security/permissions servers typically end up becoming resource intensive bottlenecks, as well as single points of failure. CKM's crypto uses public key crypto very sparingly, and the normal symmetric working key encryption processing is executed on the members' desktop computer, and not on a centralized security or permissions server. This means that CKM crypto is hundreds of times faster than traditional public key-based crypto systems, and performance bottlenecks are not likely to appear in the system, no matter how large it becomes.

A flexible key management architecture would ideally support symmetric encryption, Public Key Infrastructures, and CKM. These three technologies, blended together properly, can meet all of the requirements of secure electronic commerce around the world. This kind of encryption can effectively address emerging privacy and liability issues. The closed domain nature of an established CKM encryption boundary within a business interest can separate data effectively and easily delineate liability.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 56 of 115

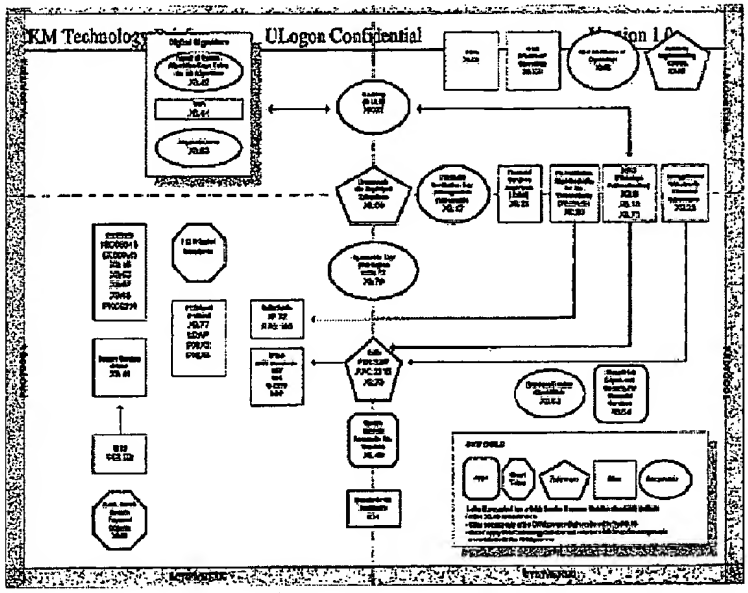
A business can now select key management methods that more closely reflect their security needs. The response to these demands focuses more on selecting the proper mix rather than selecting between competing encryption technologies.

The fine-grained, object-based encryption capability of CKM provides confidentiality to the millions of objects in an organizational database of information, and allows large organizations to put their mission-critical information assets directly on the network for even more efficient access by their thousands of employees, partners, vendors and customers. This in turn allows a complete severing of the dependence on paper-based information transmittal and storage, which in turn will finally lead us into a true electronic commerce future.

Appendix A: Standards

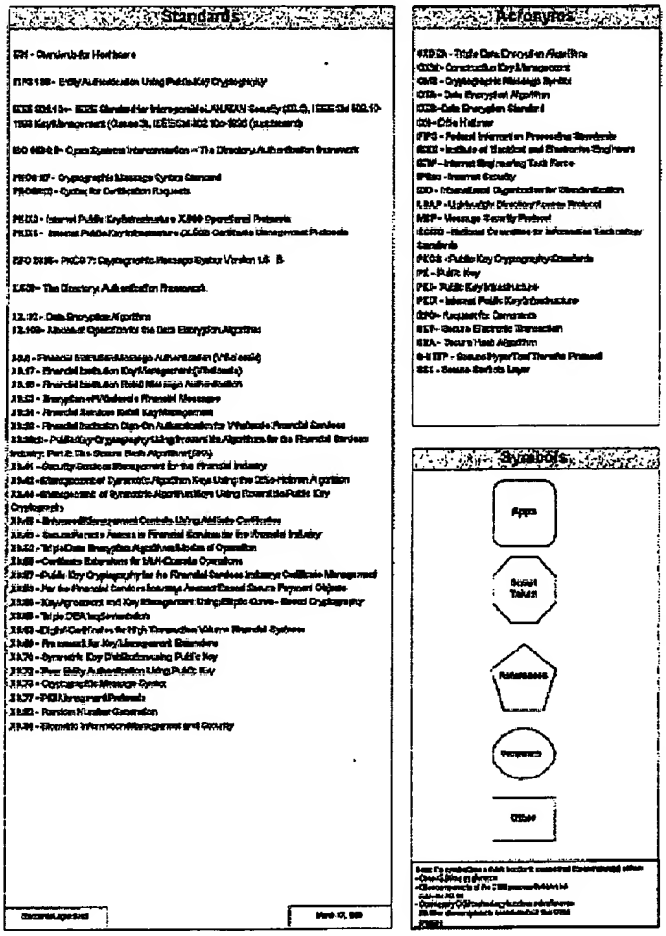
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 57 of 115



6/28/00 Page 36 Ulogon.com

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

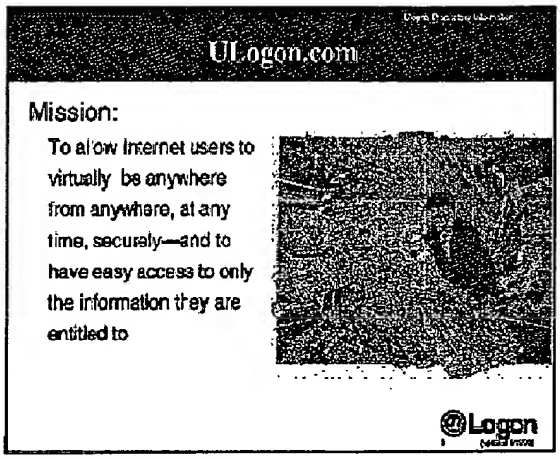
Appendix B: Export Considerations

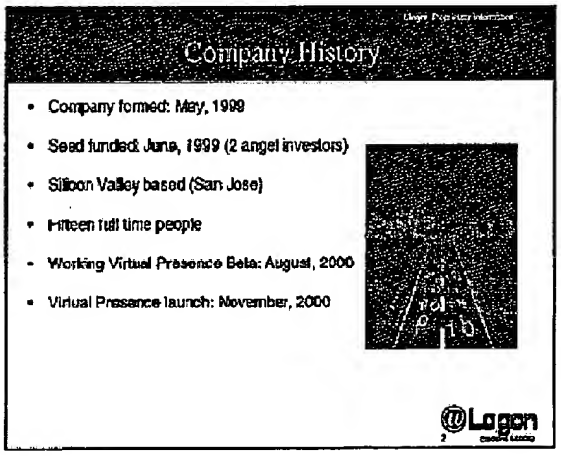
The White House recently announced a relaxation of US encryption export policy. Although specific regulations have not been issued, the following rules are anticipated:

After a one time review and approval, "commercial" encryption products with any key length may be exported without restriction to customers in most countries. There are some restricted country destinations, mostly for national security reasons. An annual reporting to the US Department of Commerce listing the identity of foreign purchasers may be required. See the Department of Commerce, Bureau of Export Control, http://www.bxa.doc.gov/Encryption/Default.htm on the web for further detail.

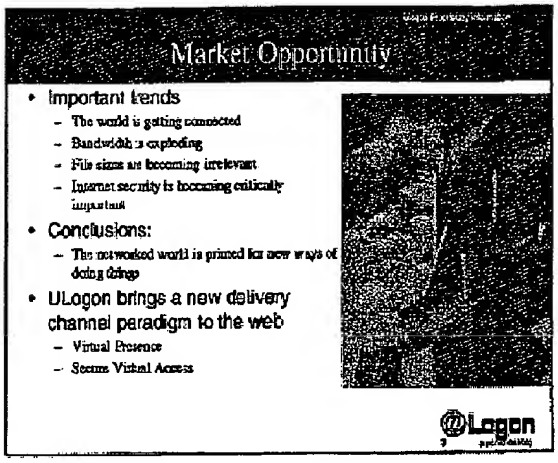
Since CKM encryption technology features 100% key recovery by the system owner, TECSEC has been granted an unrestricted export license for its CKM-2000 product line—except to prohibited country destinations. TECSEC's CKM-2000 family of products uses Triple DES algorithms and up to 392-bit (symmetric) key length. Based on CKM's 100% key recovery feature, it is believed that future CKM products, after one-time product reviews, may be exported with any key length and any algorithm.

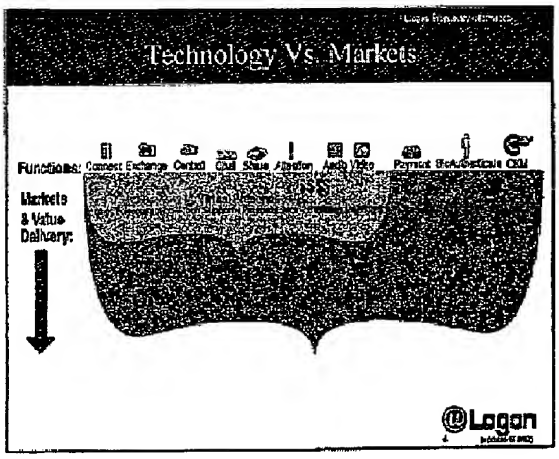
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



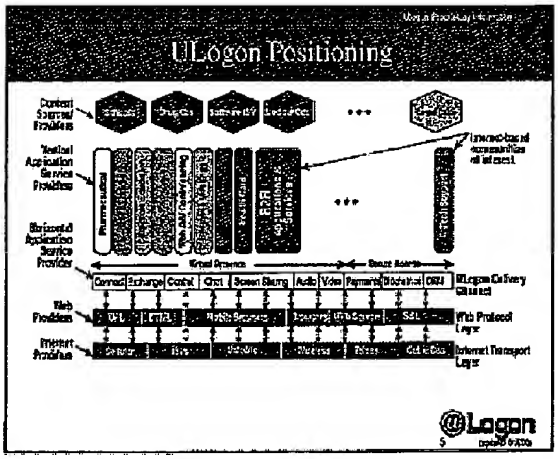


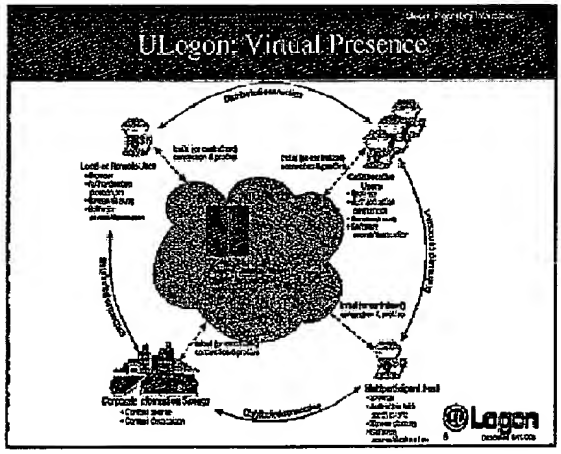
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



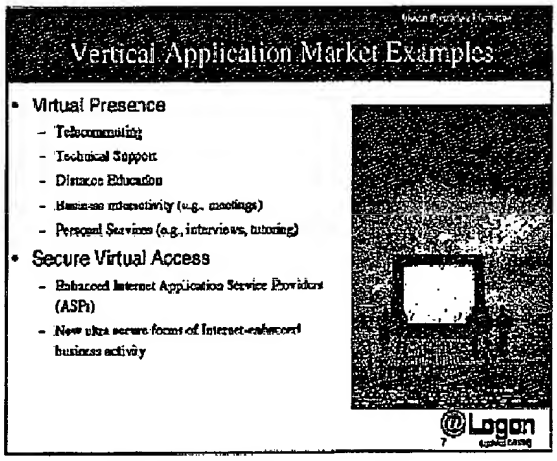


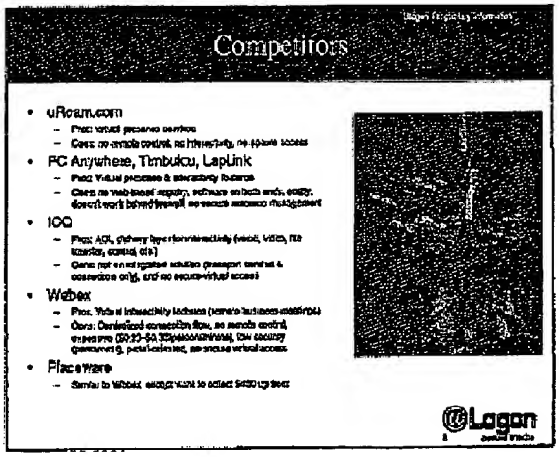
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



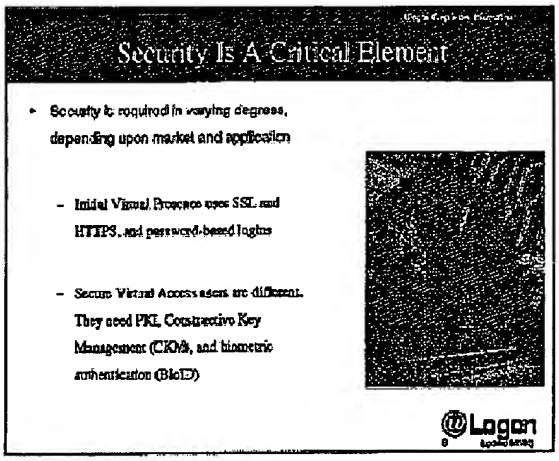


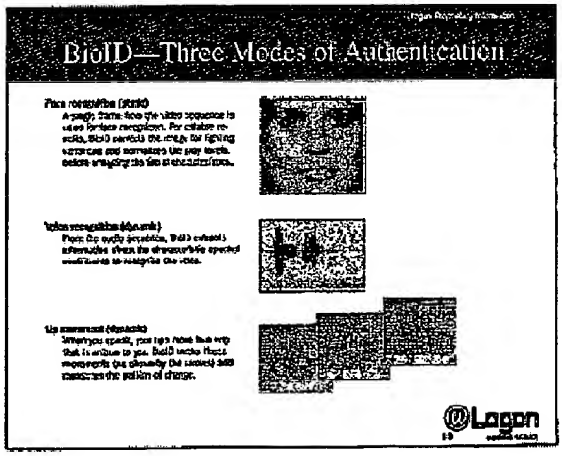
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



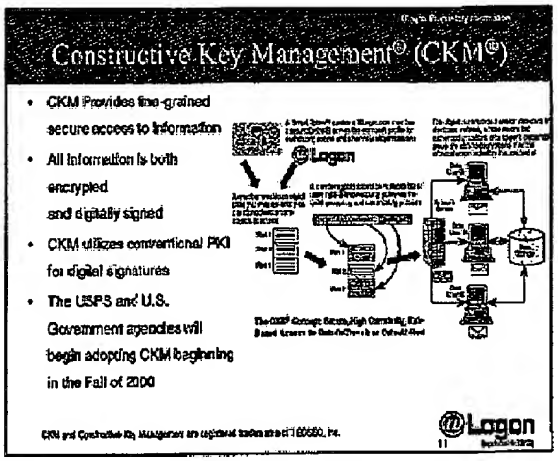


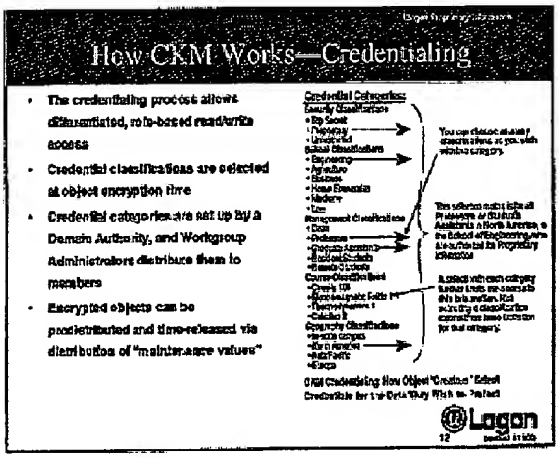
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



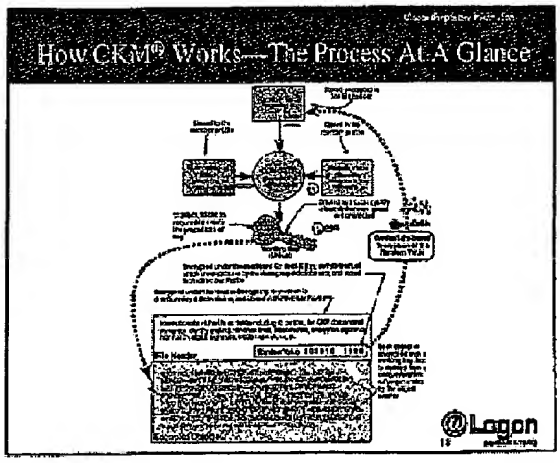


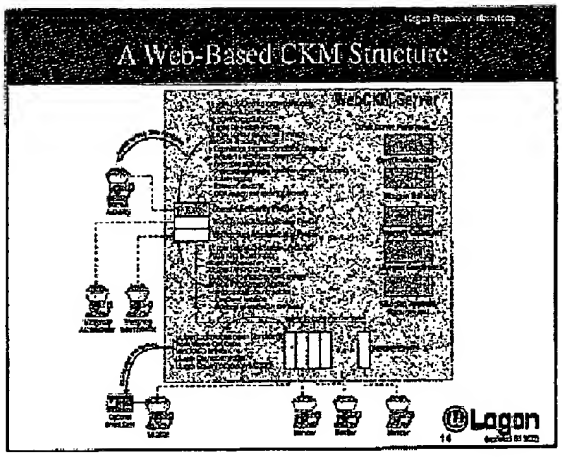
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



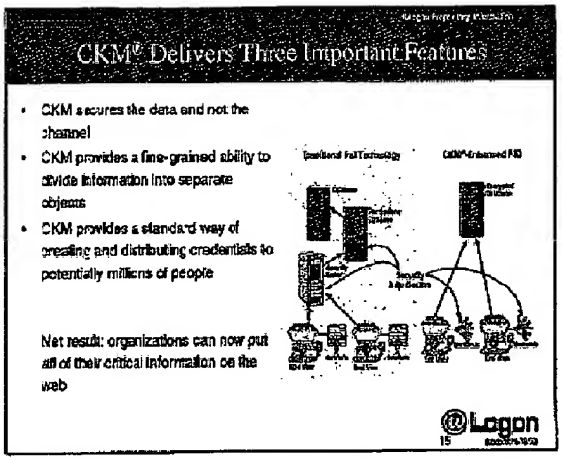


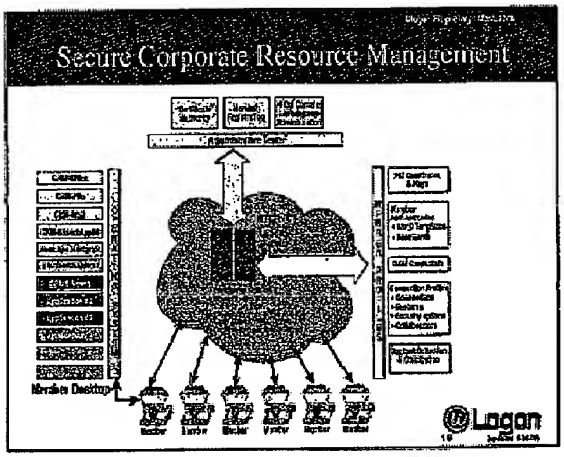
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



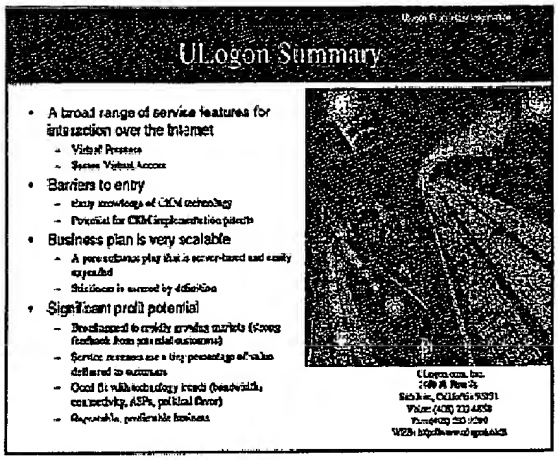


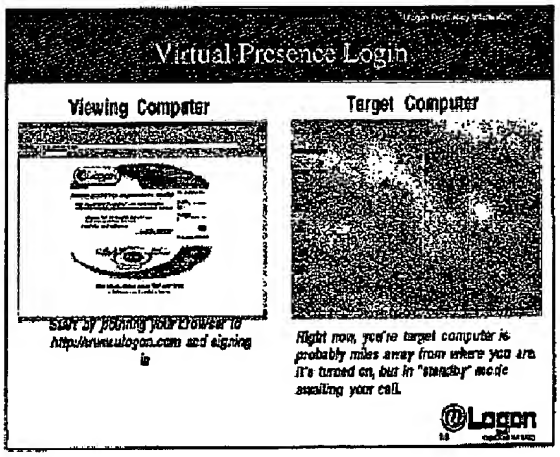
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



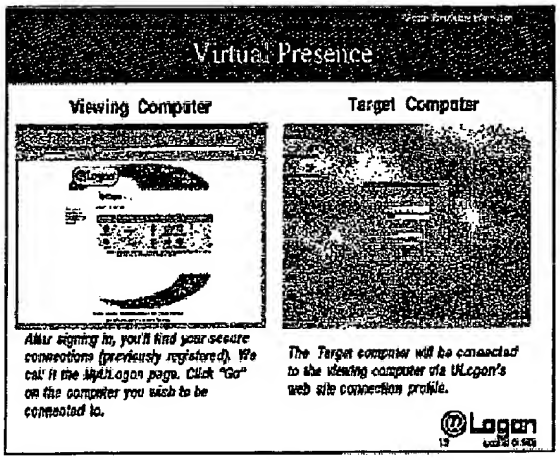


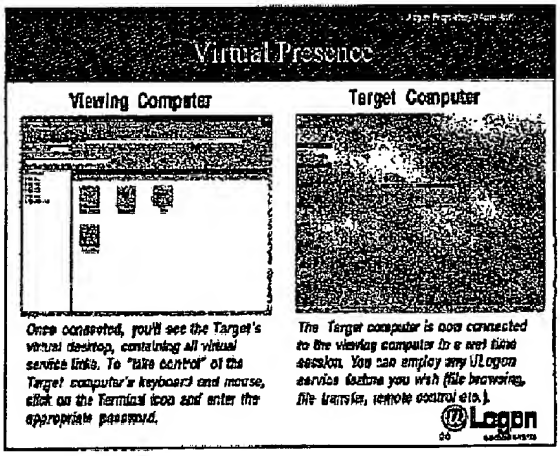
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



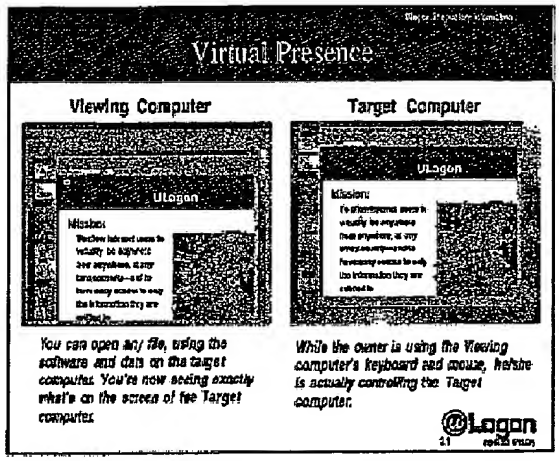


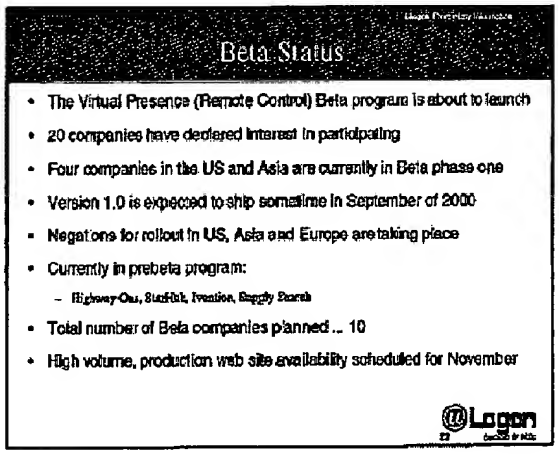
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



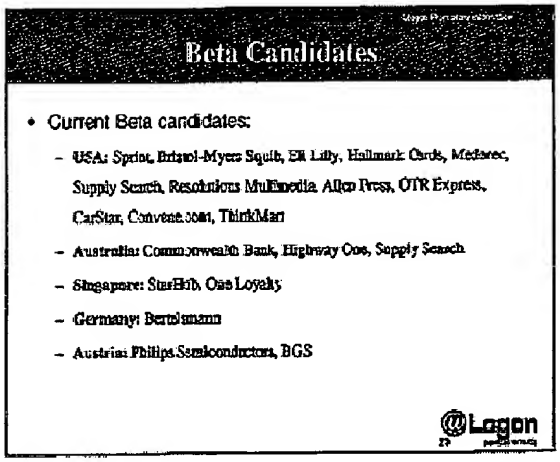


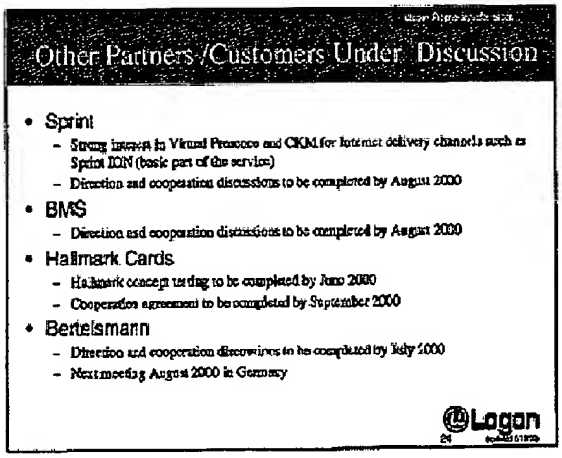
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



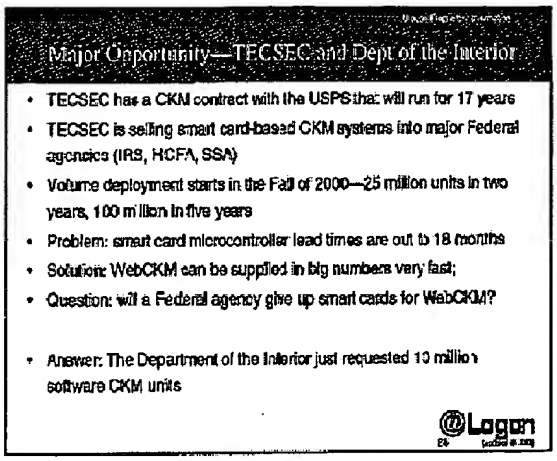


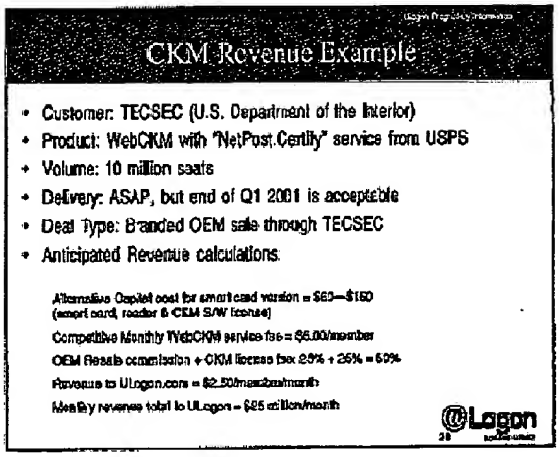
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



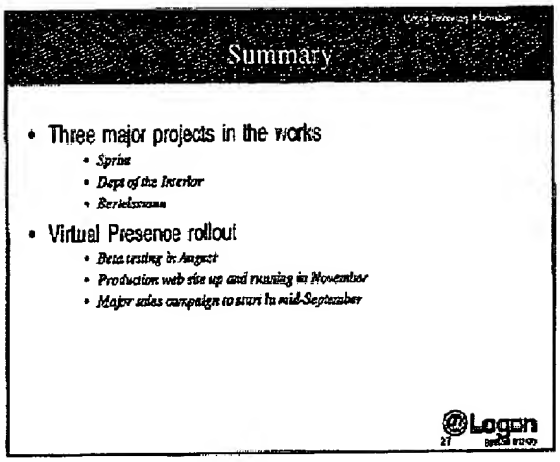


Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

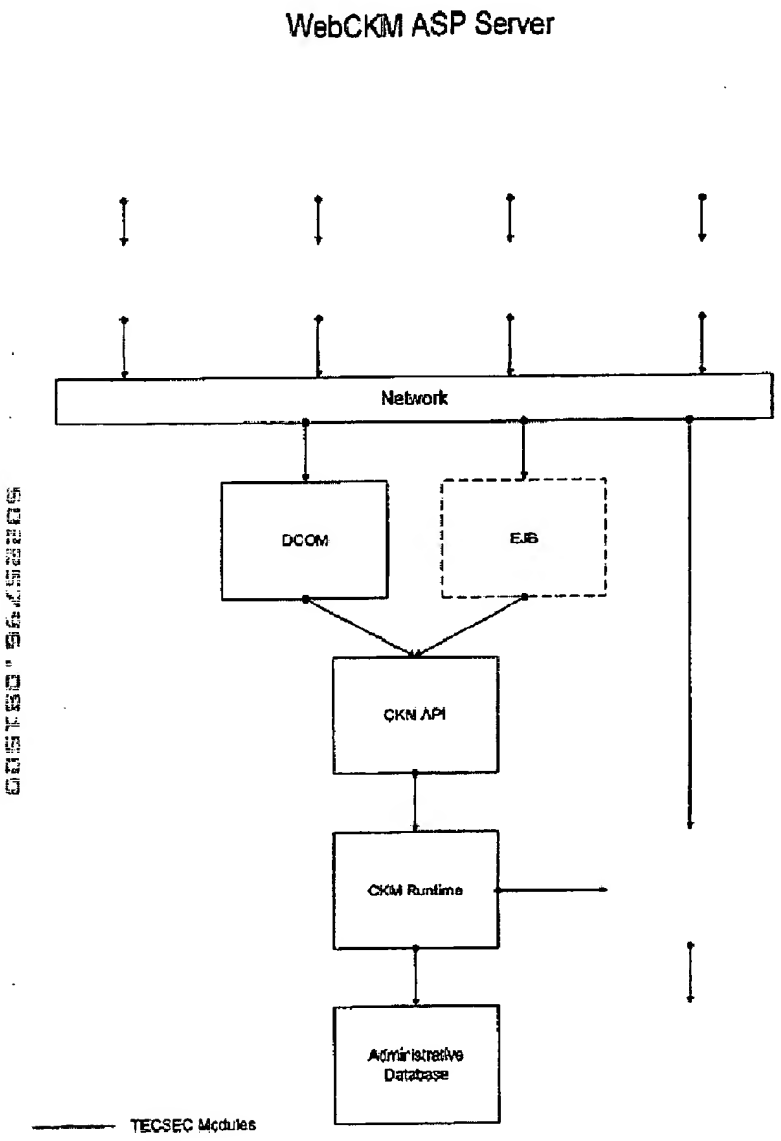




Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

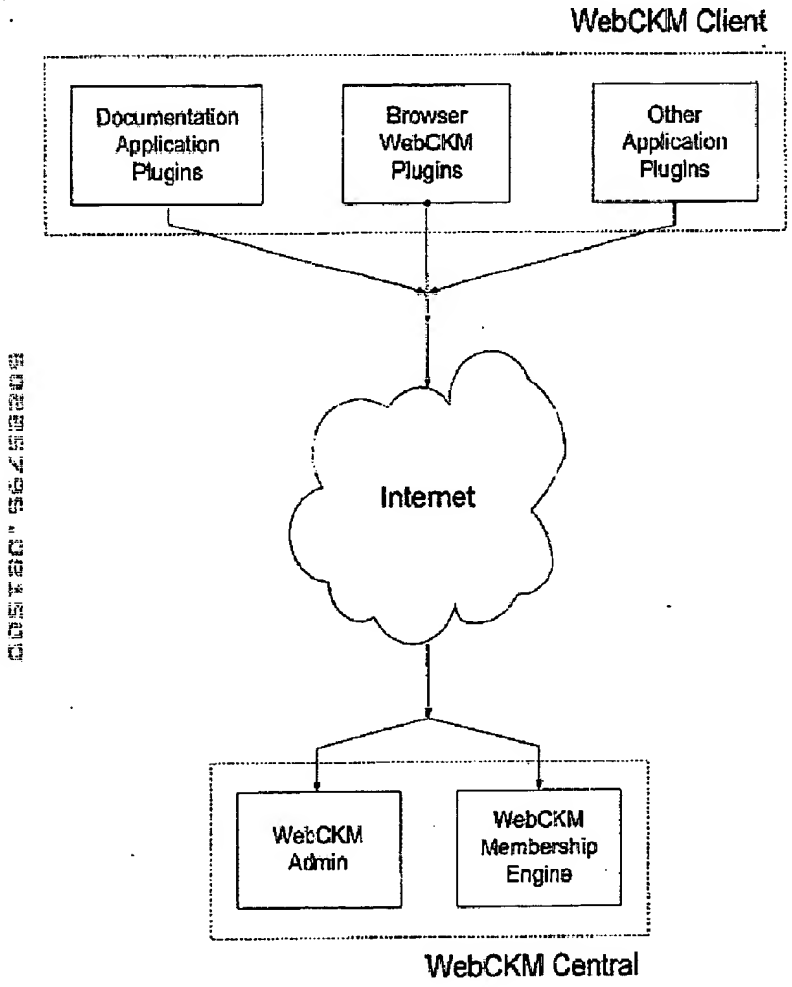


Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

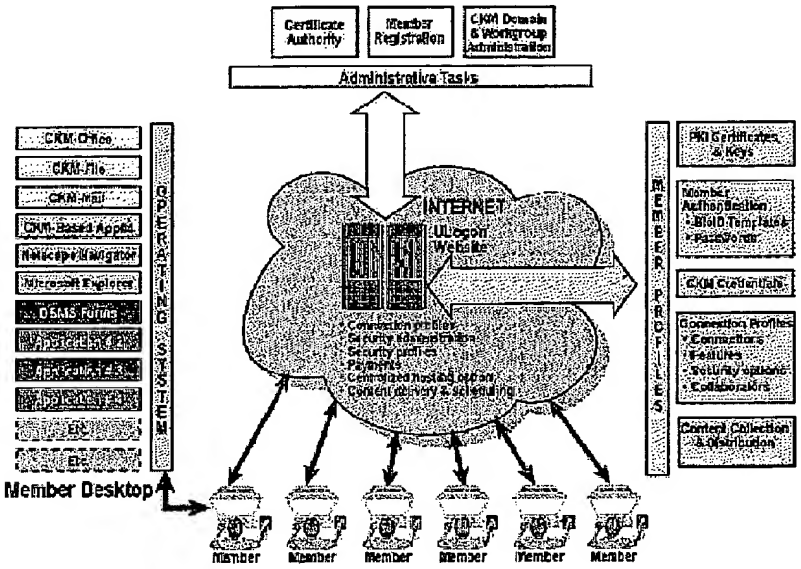
WebCKM Architecture



Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Exhibit B: Internal Disclosure Document Dated May 20, 2000

WebCKM:
A Technology Brief



VERSION 1.0 (5-20-00)

@Logon

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 77 of 115

TECSEC® Incorporated
1953 Gallows Road, Suite 220, Vienna, VA 22182-3534
Tel: 703-506-9069 Fax: 703-506-1484
www.tecsec.com

Ulogon.com, Inc.
2460 N. First Street, San Jose, California 95131
Tel: 408-232-4859 Fax: 408-232-9210
www.ulogon.com

Table of Contents

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 78 of 115

1. Introduction

At present, the commercial electronic commerce world seems committed to public key-based (asymmetric) cryptography for its digital signature and key exchange needs, and symmetric cryptography for actual bulk encryption of information.

Public Key Infrastructures (PKIs) are very good for moving information from point A to point B securely, and for providing secure authentication and non-repudiation. However, modern PKI technology still does not completely satisfy the problem of properly accessing the information once it is safely in residence at point B. This is a particularly important problem for one critical class of users: large organizations such as government agencies, educational institutions and corporations, where thousands of users need instant access to millions of pieces of information—but where each person should only have access to the information to which he/she is entitled.

Consider this problem: a specific view (report) of selected data fields in a large database contains critical pieces of information that 208 people in the organization need to electronically access throughout the month in order to do their jobs. Two people are responsible for updating (writing) the information based upon a periodic analysis of other data, but the rest are only authorized to read specific subsets of the data fields contained in the view. Thousands of other people in the organization are not authorized to access this data view, but in many cases are authorized to access other data views in this same large database. How does the organization make the information available to the people that need it, while still denying access to everyone else?

PubEc key crypto technology may provide security for transporting this data, and authenticating the people who want to access it, but it does not solve the problem of differentiated access to data fields for those 208 people.

> One way of solving the problem is to have a second database field containing the names (or other identity) of the people authorized to access each data field, along with a third field specifying whether each person has read, write, or read/write access. But this approach, if applied throughout the database, would make it impossibly large, and it doesn't work for non-database information that is kept on other servers (e.g., memos, reports, spreadsheets, pictures, etc.).
>
> A variation on the above is to build a special security server called a *Permissions Server*, and keep access rights for all users in its security database. Thus, when a user requests information from a specific view of the data in the corporate database, the requestor is first sent to the permissions server, where he/she is authenticated and the view request is logged. The permissions server then checks the requestor's access rights in its own secure database, retrieves the information from the corporate repository and presents it to the user. However, the drawback to this approach is that the permission server is a single point of failure as well as a performance bottleneck, as all people accessing data must queue up to the permissions server and typically perform one or more public key authentication steps—each of which is a computationally intensive task that substantially reduces system throughput

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 79 of 115

Another approach to solving this problem would be to encrypt each field and send all 208 people the appropriate symmetric encryption keys, and eliminate the permissions server. However, this solution will also grow to impossible key management proportions if applied to all of the millions of data fields and thousands of people who need access to them.

Still another approach—and the one currently in use at many government agencies—is to maintain multiple databases of portions of the same information, and allow classes of users to have password access to specific databases (e.g., an administrative database, an executive database, a scientific database, a legal database, etc.) This approach provides for data separation and very "large-grained" conditional access for a small number of functional groups, but is expensive to set up and maintain because of the excess duplication.

This need for "fine-grained" differentiated access is generic to large organizations and is not well solved by conventional PKI-based techniques. Traditional PKI systems have three major limitations:

- **Coarse-grained access.** Public key systems do not provide a good one-to-many solution to accessing parts of an information repository. If a member has the access rights to read a file, document or database view, he/she has the right to read *all* of it, and not just some of it. The ideal access control technology would allow different people to somehow view different parts of a single report, plan, database query, or financial spreadsheet, and deny them access to other parts. Traditional PKI cannot do this.
- **Centralized security adjudication.** Public key systems have a negative impact on computer system performance because of the computationally intense nature of public key exponentiation, coupled with the centralized nature of the security checking. When security servers or permissions servers are used to authenticate and police user information access, as the number of users and pieces of information in the system grow, they invariably become performance and single-point-of-failure bottlenecks—they simply do not scale gracefully.
- **No standardized credentials.** PKI systems do not comprehend the problem of providing credentials to people that would define their access rights to information. That is, a traditional PKI system can authenticate someone, but cannot easily solve the question of what information in the corporate repository that person is entitled to either create or access.

But now, TECSEC Inc. has invented a new distributed cryptographic key management technology that can efficiently solve the differentiated information access problem, and thus provide the final piece necessary to satisfy both industry and government with regard to electronic information access—and it is exportable with any crypto algorithm or key length. TECSEC has several patents on this technology, which is called CKM® for Constructive Key Management®, and is partnering with Ulogon.com, who will build a web-centric CKM security service ("WebCKM") that will be available to all customers on a monthly "rental" basis.

Currently, the United States Postal Service is evaluating CKM technology and a multi-year contract with TECSEC to provide a new CKM-enabled™ certified electronic mail system (internal code name of "NetPost.Certify") which will be used by millions of U.S. companies to transmit

mandatory governmental reports and other information to Federal agencies. Meanwhile, other large governmental agencies have discovered CKM technology, and are queuing up to use it for their own internal information access needs.

The purpose of this paper is to provide the reader with an overview of the CKM technology and its applications via a WebCKM security service from Ulogon.com. This paper defines concepts that are being developed and deployed in products from TECSEC and Ulogon.com. See www.tecsec.com and www.ulogon.com for more details concerning current product offerings.

The assumptions made in construction of this technology overview are:

- The reader has a fundamental understanding of asymmetric (public-key) and symmetric cryptography. If this is not true, send an email message to wbsweet@ulogon.com and he will send you an executive tutorial on cryptography that is easy to absorb and that will allow you to understand the underlying cryptography behind CKM.
- No inference should be drawn that TECSEC is representing CKM as having approvals by governmental or independent bodies other than those stated herein, including current approvals to key US Government classified information.
- This paper is a summary and significant details have not been included. Should a reader need to have a more detailed explanation regarding CKM or its potential for a specific application, please contact TECSEC Incorporated or Ulogon.com.

1.1 CKM Technology: A Fast Overview

CKM is a distributed cryptographic key management system consisting of one or more domains. Workgroup Administrators determine which members will be allowed to participate in each domain by issuing profiles to each member. Contained within each profile are each member's access rights that allow him or her to participate based on their role in the organization.

The key used to encrypt a data object in CKM is a symmetric key called the working key, typically a 3-key triple DES key. The CKM process employs three key values that are used to construct the working key: a Domain (key) value, a Maintenance (key) value, and a Random (key) value. In the most recent version of CKM—Version 5.0—the maintenance value can also be selectable as one of multiple different values.

The Domain value is used as a system key that gives system access to everyone in the domain. (In large organizations, domains can be linked together via trusted relationships, so no organization is too large for CKM technology.) Maintenance values are used to control domain membership by periodically updating the Domain value to all authorized members. This process enables Workgroup Administrators to eliminate undesirable members from future access to the system by simply updating the maintenance value to only currently authorized individuals. It also allows precise time frame control over access to data for archival researchers, since they can be given only the maintenance values for the time period(s) to which they are allowed access. This vastly simplifies the typical public key infrastructure problem of publishing and maintaining a certificate revocation list.

The third value used to create a working key is the Random value. A new random value is automatically generated each time an object is encrypted, making the working key a one-time key, unique to an object. The working key itself is not stored, but is created at the beginning and discarded after use. It is subsequently recreated when needed, but only by members with the appropriate credentials.

To segregate access to data among different groups of authorized members, the random value is further protected by encrypting it with other keys, called "credentials." Applying credentials to data to be CKM encrypted defines the readership for each object. Only those with all the credential key pieces corresponding to all the credentials used in encrypting that object can decrypt the random value necessary to decrypt the object.

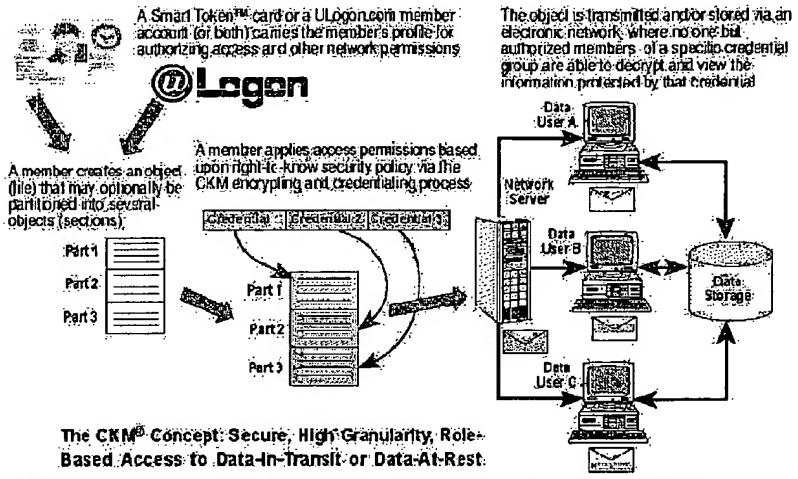
A member's profile, containing their credentials, the Domain and Maintenance values, the header encrypting key, algorithm access permissions, and domain-specific policies is contained in one of two places: either on a removable cryptographic token (e.g., a smart card), or on a central ULogon server profile maintained for each member and available over any Internet connection.)

CKM allows the distribution of encrypted objects to a broad audience where the distributor knows neither the identity nor the related access rights of each member of the audience. This provides the basis for the secure broadcast and storage of sensitive material over a network. New members to the audience are authorized according to their credentials as well.

In short, CKM allows organizations to do something they could not do before: make their repositories of critical information available to members over the Internet—securely and efficiently.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 82 of 115



The CKM® Concept: Secure, High Granularity, Role-Based Access to Data-In-Transit or Data-At-Rest

For example, sensitive corporate documents can be encrypted using CKM and placed on a company Intranet web server—without a centralized security or permissions server. Those employees with the appropriate access rights to individual documents may access each document (object), and each object may contain other objects within itself. Thus, users can access documents or parts of documents, and that access may be further constrained to read, write, or read/write permission. A single document or file may have as many objects within it as are required by the natural flow of the data within the organization.

Another example is a confidential-by-sensitive database containing medical information. Using CKM, a specific view of a selected set of fields—or subsets of the fields in that view—can be encrypted using differently credentialed random values. Doctors with one set of credentials could view a subset of a query report that contains relevant medical information, whereas administrative people could view the administrative information such as health care plan information, employer identity, etc. Administrators would be denied access to privacy-protected medical information such as a diagnosis (e.g., AIDS), and doctors would be denied access to financial information on patients they are not entitled to.

CKM is designed to be deployed as a secure system. This means employing two-factor security to protect the credentials, critical cryptographic protocols and private and secret encryption keys. With a smart card, the two factors are something you have (the card) and something you know (the PIN). With WebCKM, the two factors are something you are (a biometric authentication) and something you know (a PIN). Since a CKM system profiles are either protected by a secure smart card that can be removed and secured on the person when the member is away from his

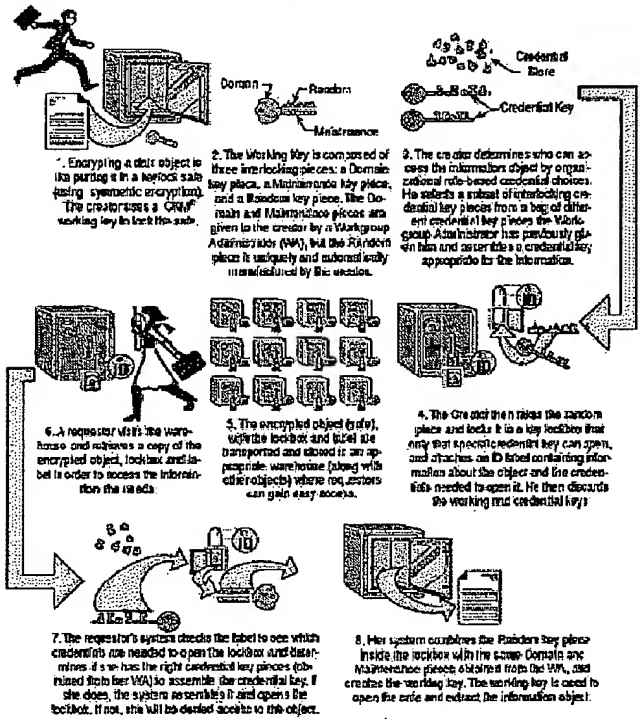
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 83 of 115

computer, or kept inside a secure network server and available only via biometric authentication, (Ulogon.com), attackers have little capability to attack.

1.2 A Graphical Analogy

The following graphic illustrates an analogy to CKM that shows the roles of Domain, Maintenance and Random (key) values, as well as how credential keying materials are applied to construct and use the working key at both creation and access time.



A CKM analogy to locking up and accessing data objects

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

2. CKM Technology Details

Constructive Key Management (CKM) is a process by which an organization can manage the flow of and access to information at the basic object level. CKM is a cryptographic key management technique that embeds access attributes and other selected parameters within the object itself. The architecture is a flexible key management system that incorporates the strengths of both asymmetric and symmetric encryption elements, adding in the unique CKM techniques that bring the fine-grained role-based differential access. Included in the architecture is an encryption key generation process based on two sets of key types: working keys and credential keys. Working key values, credential key values, a combiner process to assemble these values and key components, and an infrastructure to support the distribution and management of the generated elements is what CKM technology is all about.

CKM is a key management architecture that is available in both symmetric and asymmetric models. The CKM trust model is based on a suite of financial community standards—the ANSI standards. The founding CKM standard is X9.69, "Framework for Key Management Extensions" for which the CKM design and infrastructure architecture is modeled. Key recovery is inherent in the design since CKM allows the System Owner 100% recovery of each encrypted object, and no third party key escrow is required.

The CKM key management architecture may be viewed as a whole system's identification, authentication, access control, and encryption cycle supported by a management infrastructure.

Some terminology is needed to understand the underlying process. The key used in the encryption of an object is called the *Working Key*. It may be used as a session key or a message-encrypting key that is required by a symmetric encryption algorithm such as 3DES. The working key, constructed from several pieces of information (called values), is used to initialize a symmetric key encryption algorithm, and is then discarded. The same pieces of information used in constructing the working key for encryption are used to reconstruct the working key for decryption. The function that combines the values to create a working key is called the *CKM Combiner* and is central to the CKM encrypting process. Member identifications, keying information and credentials are stored in a large file called a *Member Profile*, which typically travels with the member in a smart card or is accessible over the Internet in a central Ulogon.com server file.

Access control is provided in CKM by applying credentials in the encryption of keying information that is embedded in the object file header attached to the object. Asymmetric values are associated with each credential set. Read/write separation is cryptographically available with such an asymmetric key design. Read access is equivalent to decryption rights and write access is equivalent to encryption rights.

In addition to access control, a broader key management strategy may include a configurable identification capability and a third-party trust authentication capability as illustrated in the figure below.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 85 of 115

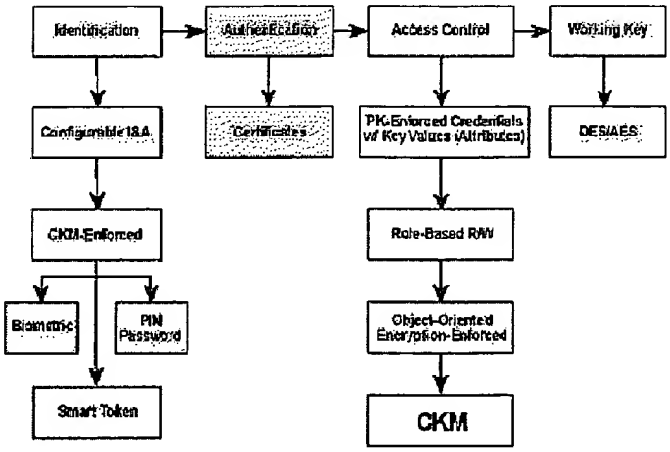


Figure 1: A flexible key management strategy

Credentials may be associated with an application that defines one or more member identity elements such as a biometric function, a smart card identity, or a PIN/Password. CKM is used to bind the identity elements to an encrypted object through an encryption process. The I&A (Identification & Authentication) object may consist of a Public Key Infrastructure (PKI) functions that can authenticate the member to the network and other members, and other functions that may need to be stored secretly and which are included in a Member Profile. The essential part of PKI is a certificate that includes a verifiable digital signature, which is itself a mathematical hash of information that is then encrypted through an asymmetric (public key) process. The PKI authentication support is managed through either the smart card or the central Ulogon.com server.

The figure below illustrates a Ulogon.com server and its interaction with a configurable Identification and Authentication (I&A) process:

1. Two types of asymmetric key pairs identified as Global and Membership;
2. Payment functions; and
3. Data that acts as a physical access function.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 86 of 115

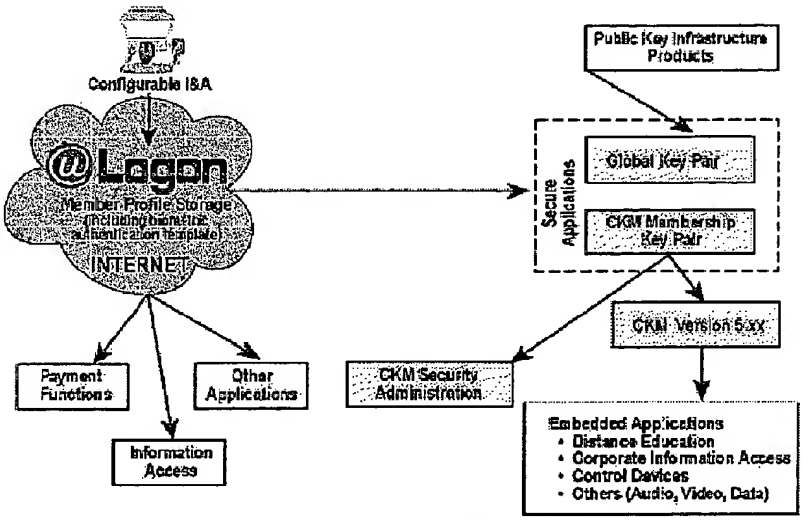


Figure 2: ULogon.com: avenue to comprehensive security

TheULogon.com Member Profile is used as a bridge to multiple authentication and encryption platforms with varying degrees of encryption enforcement and binding.

2.1 CKM Domain

Under a role-based access control system, rights and permissions are assigned to organizational roles, rather than to each member. As members' assignments change, their rights and permissions are changed to reflect their new roles. CKM, with its method of using credentials reflecting information flow and boundaries, is a preeminent example of a role-based system. The CKM design offers a method to anticipate data boundaries without knowing member identities.

CKM Administration is based on several core concepts that apply to any CKM setup—even if some are transparent. This section provides an introduction to each of these critical concepts.

The highest unit of organization in a CKM System is the *Domain*. A CKM Domain is a unique, independent entity that includes all CKM resources needed to function on its own. CKM security policies, procedures, and roles are all determined at the domain level.

Although it is the largest unit of organization supported within CKM, domains are fully scalable to a wide variety of needs. A CKM Domain may be as large as an entire enterprise or as small as a single member. One type of application might, for example, establish a unique domain for each

member, while small businesses would likely establish a single domain for the company, and large enterprises would establish many domains for major divisions, different locations, or other organizational structures.

While domains are freestanding and independent, they do not need to be isolated. CKM Domains may share access rights and privileges with other domains in a *trusted* relationship. Additionally, members may participate as members of multiple domains even if a trust relationship between the domains has not been established. The CKM Domain may have a direct relationship with a PKI Certificate Authority (CA), if so desired.

2.1.1 Trusted Domain Relationships

A CKM Domain may provide specified access rights and privileges to members of another domain by establishing a trust relationship. The trust relationship is established when one domain provides a subset of its CKM Credentials to another domain. Credentials are shared *only* at the domain level and may not be sent directly to members of another domain until a trusted relationship has been established. Once trust has been established, the second domain maintains and distributes "imported" credentials using its own methods and policies, and these credentials are stored in the same *Member Profile* as part of the member's credentials. Once distributed, members of the second domain may use the imported credentials to share information with members of the external domain, but they continue to be bound by the policies and procedures of the domain in which they hold membership—their *LogOn Domain*. If a PKI CA is included in the key management architecture, a third-party authentication model may be added to the overall trust relationship.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 88 of 115

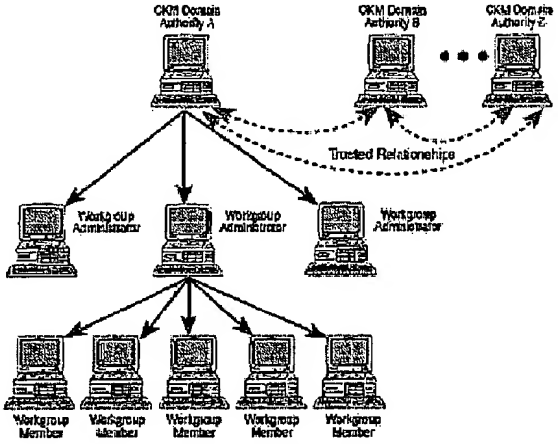


Figure 3: The CKM Hierarchy

2.1.2 Untrusted Domain Relationships

An individual may be a member of several CKM Domains regardless of whether the domains have established a trust relationship. That is, two or more domains may grant membership independently to the same individual. In this case, CKM sees the single individual as several members—one for each domain. In this type of untrusted relationship, the member will log onto each domain independently, use separate *Member Profiles* for each domain, and possess credentials only to access information within that domain (and with its trusted domains.)

Note: Some storage mediums (such as Smart Cards) currently do not have sufficient space to hold more than two or three Member Profiles. Therefore, the ability to log on to much more than two or three domains may require that additional cards be carried by the member. As time and semiconductor technology moves on, however, it is anticipated that smart card memory sizes (currently a maximum of 32KB) will increase substantially, thus providing room to carry a significantly larger number of Member Profiles. The WebCKM system, since it depends upon a central server to hold all profiles, does not have any practical limits on the number of profiles or the size of any corresponding data in each member's "connection profile."

2.1.3 Domain Authority

The Domain Authority (DA) provides top-level management to a CKM Domain. Although some decisions must be made by the person or persons assuming the responsibility of the Domain Authority, many DA functions may be automated.

Typically, the Domain Authority sets up the domain by performing the following functions:

- Names the domain and creates its unique *Domain Value* (used in cryptographic functions)
- Establishes and updates a number of *Maintenance Values* (used for revocation and to control information access to specific time windows)
- Sets policy defining the outer parameters of CKM use, including whether member Profiles are hard disk-resident, server-resident (WebCKM), or token-resident.
- Establishes and digitally signs the role-based *credentials* used by CKM to cryptographically enforce access control to information
- Selects and optionally renames the cryptographic algorithms available in the domain
- Selects and configures Identification & Authentication objects available in the domain
- Registers *workgroups* and their administrators through which credentials are distributed
- Digitally signs individual membership keys and authorizations related to CKM enrollment
- Registers and digitally signs CKM-enabled applications
- Creates and distributes *Workgroup Profiles* defining a subset of credentials, algorithm permissions and policy settings available to each workgroup
- Determines trust relationships with other domains

CKM allows members to receive credentials, policy settings, and algorithm permissions only if signed by the Domain Authority—even if some of these values are imported from other domains. Members are bound to the Domain Authority via the DA's CKM Membership Key and certificate issued to the member. The DA's CKM Membership Key is then used to verify the DA's signature when receiving credentials and related material.

2.1.4 Domain Profile

A Domain Profile refers to all credentials, policy settings, and algorithm permissions established by the Domain Authority and available within the domain. The Domain Profile also includes the domain's name and value, the maintenance value, and other information identifying the domain.

2.2 CKM Workgroups

A CKM Domain consists of at least one and usually several workgroups. A workgroup clusters members (or smaller workgroups) based on common needs and rights to information. Workgroups are often established to parallel departments, locations, projects, or other natural organizational subdivisions.

2.2.1 Workgroup Administrator

Workgroups are typically managed by a Workgroup Administrator (WA). The responsibilities performed at this level may be by a person interacting with software, or may be automated in part or in full. These responsibilities typically include the following:

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 90 of 115

- Refining policy settings (as allowed by the DA) to provide further restrictions than those originally granted to the Workgroup by the Domain Authority
- Registering the individuals who become the members of the Workgroup
- Assigning subsets of credentials and algorithm permissions available in the Workgroup Profile to individual *Member Profiles*
- Signing, distributing and updating *Member Profile Updates* to Workgroup Members

2.2.2 Workgroup Profile

The Workgroup Profile contains all credentials and algorithm permissions available for distribution to the members of a specific workgroup. It also includes the policies governing the workgroup's use of CKM. Workgroup Profiles may differ from other profiles in the same domain—defining the unique rights and needs of each group. Workgroup Profiles are created by the Domain Authority.

2.3 Member Profile

A *Member Profile* includes the credentials, algorithm permissions, and enforced policy settings assigned to an individual by a Workgroup Administrator. The Member Profile also includes the individual's private asymmetric CKM Membership Key used to decrypt profile and other membership information sent to the member by the Workgroup Administrator. The member's "public" CKM Membership Key is retained by the Workgroup Administrator and is not posted for public use as in a PKI. The Member Profile also includes the "public" CKM Membership Keys of the Domain Authority and Workgroup Administrator. Also, in WebCKM systems, it will also include one or more global and workgroup membership PKI (individual) private keys and digital certificates used for encryption or signing in WebCKM and other cryptographic systems. See Figure 2.

Members may receive profile and membership information from the single Workgroup Administrator whose Membership Key has been issued in the Member Profile. All updates to Member Profiles are signed by the Workgroup Administrator (WA) and must be verified by the WA's CKM Membership Key held by the member.

Members may be assigned to a different Workgroup Administrator only by receiving a new WA Membership Key signed by the Domain Authority. Additionally, credentials may be updated or added to the Member Profile only if signed by the Domain Authority and verified using the DA's CKM Membership Key held by the member. In this manner, each individual is bound to a specified workgroup and a specified domain.

2.3.1 Profile Storage

A Member Profile may take many forms. It may be stored locally on a member's workstation, on removable storage such as a floppy disk, on a network server such as Ulogon.com, or on a physical token such as a smart card. The form of the Member Profile is configurable by the DA. One of the policies carried within the profile determines where profiles are allowed to reside. The

form of the Member Profile is also dynamically scalable, i.e. if the profiles are not found in the one location, then CKM will look to the next location until the installed list of locations is exhausted. If a profile is not found in any of the allowed places, then CKM will prevent the member from initiating a session.

2.4. The CKM Process

2.4.1 The Security Paradigm and Data States

Adequate security is the condition at which protective measures have been employed that reduce the risk of loss to an acceptable operational and financial level. Total effectiveness depends on the synergistic interaction of various system features that reduce threats from inside and outside attackers and/or other vulnerabilities. This synergistic interaction forms a trust model. That is, one security measure alone does not provide adequate security. Only when all are taken together does adequate security result.

Encryption is a tool that mitigates certain vulnerabilities and thus reduces risk. To form an effective information security trust model, a member must be "bound" somehow to the data he or she is authorized to access. CKM technology begins with strong Identification that is then directly bound to the encryption of objects via a credentialing process that in turn ensures the integrity and access control of the information being protected.

Since CKM is client-based, the trust model may be scaled to many members: 1) by distributing the workload to member workstations (desktops), and; 2) by making the encrypted object the basis of trust adjudication instead of a network-based server. *These are two critical differences between CKM and traditional PKI structures.* In a traditional PKI system, a front-end server protects access to the data, and the security focus is on authenticating each requesting member, both as to whom he/she is, and as to what information he/she may have access to. *With CKM, the typical PKI authentication step with a centralized security server is not required.* Once profiles have been distributed to members, encryption and decryption is controlled by individual member profiles, which typically will either reside on a smart card or a web server.

Data may be viewed at any given time of being in certain states:

1. Data at rest: data objects are in a fixed state in a storage capacity. An example of this state is a data field in a large centrally located database, or a series of documents resident on a network server.
2. Data in transit: data objects that are being transmitted in a communication channel during a period of time.
3. Data in process: data objects that are in static memory areas being manipulated by a computer operating system and/or one or more applications.

CKM can provide a key management and control scheme for both data-at-rest and data-in-transit. Data-in-process security is dependent for the most part on operating system and hardware-based control mechanisms.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 92 of 115

2.4.2 The CKM Combiner Function

The role of the CKM combiner is to create a working key from the domain, maintenance, and random values. The working key encryption process uses a standardized triple DES (3DES) algorithm. The output of the combiner function is the (3DES) working key as shown below.

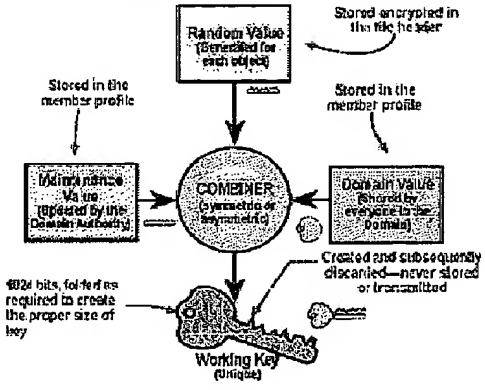


Figure 4: The CKM Combiner Function

The working key is destroyed immediately after an object is encrypted. In order for recipients to be able to decrypt the object, certain information is given to them either within an object header or via the member profile. The random value is encrypted with a key generated (assembled) by the credentials the encryptor (creator) selects. It is important to note that it is not possible to recreate the working key solely from information provided in the object header.

The working key is used with a symmetric encryption algorithm such as 3DES or a future U.S. Advanced Encryption Algorithm to encrypt the actual data object. Since the working key is destroyed immediately after an object is encrypted, information pointing to the specific data required (which a member may or may not have in his/her profile) to reconstruct and apply the values, credentials, and other functions are included in an encrypted header that anyone in the domain can open. The header-encrypting key is managed through the same distribution scheme as the maintenance value and credentials (e.g., distributed from a Workgroup Administrator's account at the Ulogon.com server to individual workgroup members' accounts at the same server), and all can be updated concurrently.

Read and write access, and the protection of the random value are accomplished through a combination Diffie-Hellman (asymmetric) process that creates random value encryption keys. Normally, symmetric key cryptography (3DES) is used for random value encryption. In the asymmetric credentialing process, a Diffie-Hellman static key pair is associated with each credential (piece) and the "public" key of each pair is used to derive keys that are then combined mathe-

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 93 of 115

matically to create sufficient keying material to encrypt the random value. A member with an appropriate set of Diffie-Hellman "public key"-based credentials may encrypt objects, and a member with the corresponding set of Diffie-Hellman "private key"-based credentials can decrypt those objects. A member with both sets has both read and write access. This process results in other parameters that are also included in the member's profile, and an additional level of assurance within the combiner functionality.

2.4.3 The CKM Header

A CKM object header must be available to decrypt an encrypted object. The CKM header contains, among other things, the encrypted random value used in constructing the working key. Since the header is encrypted with a header key known to all in the domain, the header of every object encrypted by CKM may be read by anyone in a workgroup belonging to the domain. Note that the random value is not available to those without cryptographic read permissions for *all* the credentials originally used in that specific object encryption process.

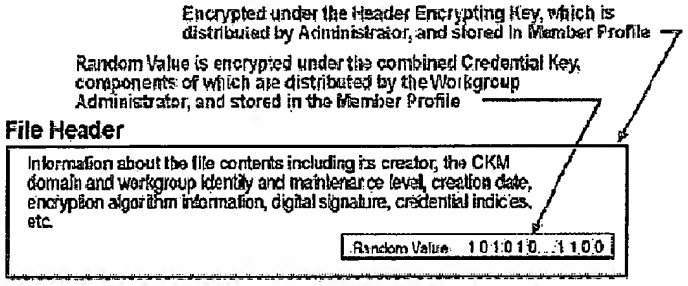


Figure 5. The File Header contains information about the file, along with the Random Value, which may optionally be encrypted with the combined credential key. The header is encrypted with the Header Encrypting Key, which all members of the domain possess.

2.4.4 The CKM Object Encryption Process

With CKM, a file or document may be encrypted with a working key. Alternatively, a component of that file or document (called an *Object*) may also be encrypted inside the main file with a working key different from the main file. With traditional PKI security methods, data objects can typically be no smaller than an individual file or database view. With CKM, however, an object can be as small as a single word within a file, or a data field within a database view (query, or report). This object-within-an-object architecture places no constraints on an organization's ability to apply CKM technology to its natural information segmentation—either when the data is at rest in a network-connected information repository, or while it is being transported across the network by several transport mechanisms (each providing a secure CKM "object wrapper" around the object being transported).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 94 of 115

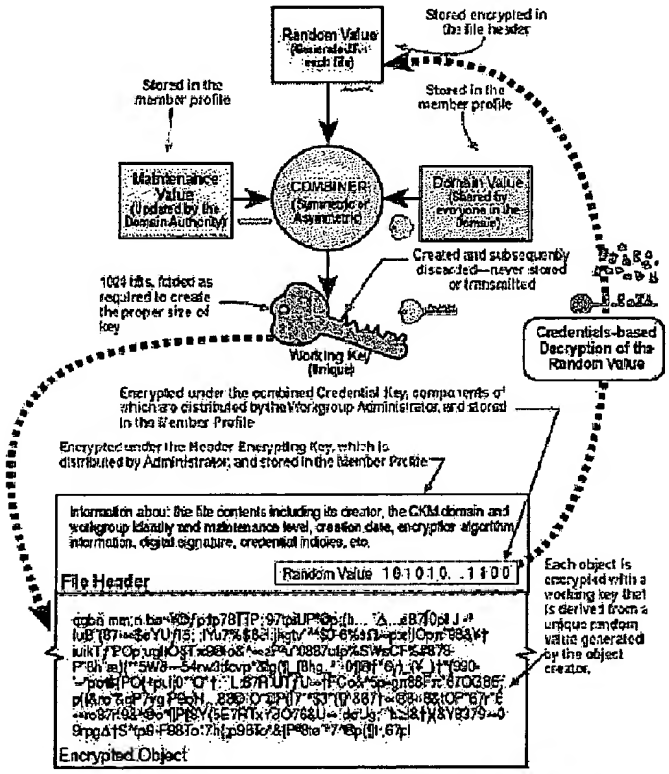


Figure 6. The detailed CKM process for a single object

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 95 of 115

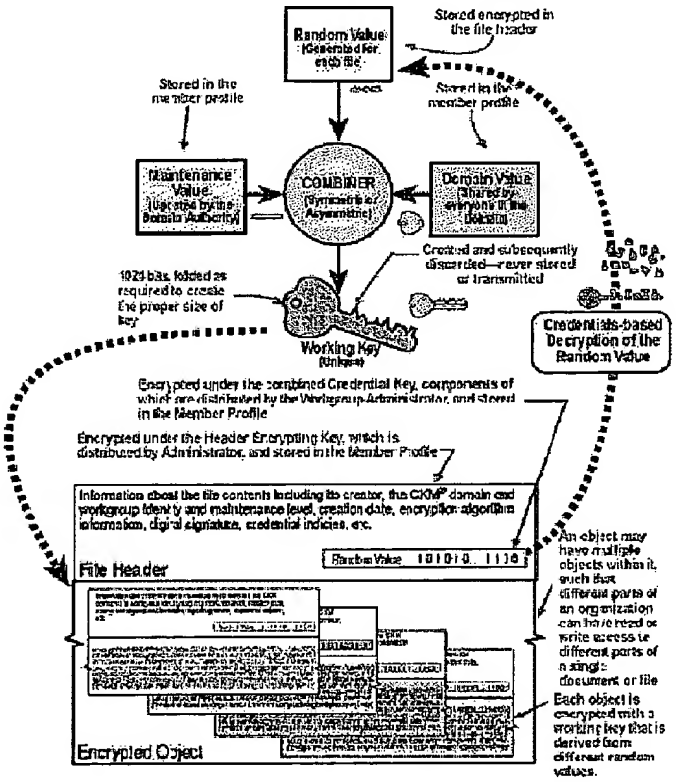


Figure 7. The detailed CKM process for multiple objects

With CKM, objects can be contained within objects. This is convenient for several reasons:

- When different people need to be granted different access rights to data objects within a document or database, each unique data group (e.g., sections within a business plan) can be designated as an object and included within a higher level object (the business plan.) In this case, lower level objects may be arranged within a higher level object in a parallel fashion.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 96 of 115

- When different transport mechanisms are used to move a data object, each may wrap the object it receives with its own CKM credentials (e.g., a local police department message, encrypted under that department's domain, then wrapped by the FBI domain on the Internet, and traveling over a State Department network, which applies a State Department CKM credentialing and encrypting process.)
- Alternatively, data objects may be organized in both hierarchical and parallel subdivisions, each architecture tracking the way in which an organization performs its mission. CKM can easily adapt its object hierarchy to fit almost any organization.

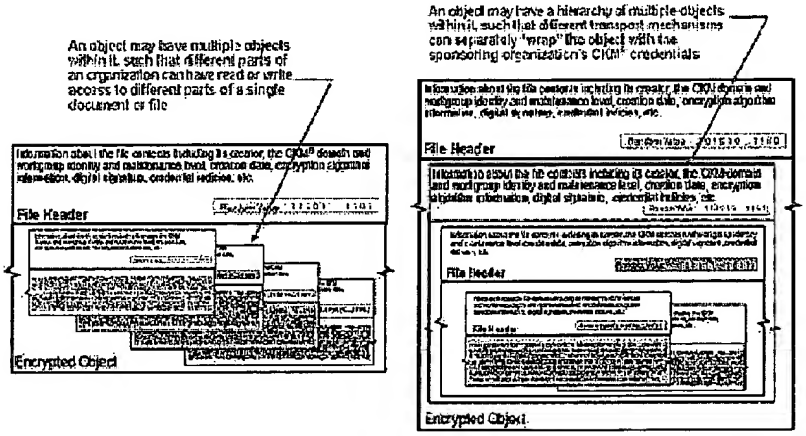


Figure 8: CKM object combinations

2.4.5 The CKM Credentialing Process

CKM is superior to other cryptosystems for many reasons, but the most important is that it allows differentiated role-based access to large databases of information. This process is initiated at the time the data is entered into the system. For example, in a large reporting document (file) with many sections, each section, chapter, paragraph (or word) can be credentialed and encrypted differently from the others, according to the roles selected for read or read/write access. A simple example of credentialing choices for the creator is shown below.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 97 of 115

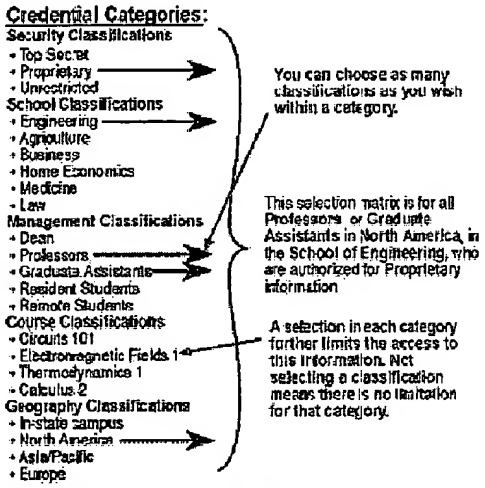


Figure 9. A simplified example of the CKM credentialing process in an educational setting

Credential categories and classifications are defined by the Domain Authority. Note that within the set of credential choices, multiple classifications selected within a category are ORed, while all Category choices are ANDed together conceptually to derive the credential keys used to encrypt the random value (e.g. [Proprietary] AND [Engineering] AND [Professors OR Graduate Assistants] AND [North America]). *All* credential categories included at the creation of the information must be available in the member profile of anyone wishing to access that information. If only one required credential category is missing, the object will be unavailable.

This CKM credentialing function brings two critical benefits to the access control problem:

- Credentials allow role-based access designations to be applied directly to a data object such that access can be controlled by the credentials held in a member's profile, thus eliminating the need for a permissions or security server;
- By providing a standardized way of creating and applying credentials that information creators can be trained to use consistently throughout a domain, CKM brings a new standard methodology that substantially enhances information access for organizations of all kinds.

2.4.6 The CKM Session

The Domain Authority sets, and Workgroup Administrators enforce session timeouts for members. Based on the security risk, the maximum idle time during each CKM session may be centrally controlled. Session timeouts are included in each member's profile and may not be reset by the member. Generally, the member is required to repeat the identification and authentication process in order to restart a timed-out session.

2.4.7 Identification and Authentication

Identification is the process of identifying the member. Authentication is the process of validating that identity. CKM profiles are encrypted with an identity process. In order to access profiles, members must provide proof of identity. This proof may consist of presenting valid User Identification (UID) along with a correct password (PIN). It may also consist of presenting a biometric scan such as facial contours, voice recognition, or lip movement while speaking a passphrase. Authentication occurs at the workstation when valid identification is presented for the profile that was issued by a Workgroup Administrator.

A Workgroup Administrator creates each member's profile. Among the data included in each profile is the member's identification. The member may not change the UID supplied by the Workgroup Administrator. Each time an object is encrypted, the identity of the profile used is placed in the header so each recipient may verify the identity of the encryptor. Trust is assumed since only a Workgroup Administrator may issue profiles and only a Workgroup Administrator may designate UIDs.

2.4.8 Revocation of Member Access

Any cryptosystem must have the means to revoke a member's access. Revocation refers to preventing access to material encrypted subsequent to revocation. It does not refer to preventing access to material encrypted during a member's period of legitimate access. Once the decision to revoke is made, new encryption access denial should be as complete and rapid as security risks warrant. CKM has multiple means to revoke members. The basic CKM revocation methods are listed below:

- Profile expiration limits provide a routine, periodic method of removing member access, just as credit cards expire. As profiles expire, they may simply not be renewed.
- Updated maintenance values eliminate access to those without the new value. New maintenance values have backward utility so that material encrypted with a previous maintenance value may be decrypted with a subsequently issued one. The DA may choose to issue a new maintenance value and not give it to certain members, thus revoking their access to future information. Periodically, new maintenance root values may be issued that do not have backward utility, thus marking the beginning of a new time period. Multiple maintenance values and multiple roots allow fine-grained control over time periods.
- Maintenance values can be used as "time release" factors for time sensitive materials. For example, course materials may be issued to a student by an educational institution, and

new maintenance values may be issued at the beginning of each week to "unlock" content appropriate for that week's study or testing.

- An advantage of a web-centric CKM system (Ulogon.com) is that member profiles can be cancelled or changed any time with virtually immediate effect. As members connect to the central site to use their member profiles to access old content or create new content, their credentials can be changed from the last access. This facility is particularly useful in responding to—or preventing—certain security attacks by outsiders and/or former workgroup members, since all an administrator has to do to forestall such attacks is cancel a rogue member's credentials. This is a more difficult problem for smart card-based systems, since a rogue member could continue accessing content up until the credentials on the card finally time out.

2.4.9 Key Recovery

Key recovery refers to the ability to recreate or retrieve working keys. CKM technology is unique in that unlike in private key escrow and session key escrow, CKM does not escrow anything. CKM provides the Domain Authority—and to a limited extent the Workgroup Administrator—with the ability to reconstruct all working keys, since the DA created all the system keys, as well as all the credentials. If the header or its equivalent is made available to the DA, the working key can be reconstructed.

This key recoverability of CKM is a critical advantage for two reasons:

First, all organizations need an ability to recover encrypted files when the primary encryption keys have been lost. Modern high strength encryption is virtually unbreakable; so locking up vital intellectual property and then losing the keys means that data would be lost forever. In typical commercial use, employee turnover, computer failures, loss of tokens, and other catastrophes happen to a significant percentage of organizations every year. Thus, it is in the organization's best financial and security interests to have a simple recovery capability in case a workgroup member loses his or her keys. CKM provides a simple key recovery capability.

Second, modern high strength symmetric encryption is subject to government control in many countries. In the United States, the export of strong encryption is regulated. These regulations are continually being revised to address the demands of electronic commerce and national security issues. TECSEC has been granted a unique export license for CKM technology. See Appendix B for more details.

2.4.10 A Word About Databases...

CKM usage with normal electronic document files is fairly straightforward. Data objects are encrypted with specific CKM working keys, grouped into object hierarchies and stored on network-available magnetic or optical storage devices for access by a multitude of members with the appropriate credentials.

Databases, however, are another problem. Because large relational databases need to conduct internal operations on the data contained within, encrypting each field can pose a problem. How can a database sort data, calculate indexes, create calculated values (from multiple data fields),

and perform ad hoc inquiries if each field is encrypted? If encrypted with CKM, how would the database know what working keys to use? Where would such information be stored? This is a case where encrypting the data for security reasons may get in the way of managing that data within a relational database.

A number of techniques have been developed to solve this problem as follows:

- Members filling out database forms for submission to the database do not necessarily need to worry about which credentials are to be applied to each field. Special templates are created which present preformatted electronic input forms for members to key in the data. Each template carries within it the index values of the preset credentials associated with each data field. Thus, clerical staff need not even know what credentials are being applied—all they know is the data is entered and sent on its way when completed, using their member profiles and their desktop systems to perform the necessary encrypting and digital signing of objects.
- CKM-encrypted data may be stored directly within the database structure. If it is done this way, database indexing must be simple (e.g., based on serial numbers) and file header information must also be kept in order for the database to decrypt data fields for internal maintenance purposes. This provides for substantial protection against hackers that might search the magnetic or optical media with analytical tools. However, it makes ad hoc searches of the data difficult to conduct.
- One approach is to decrypt all data coming into the database and store it within the database structure as plain text (non-encrypted). Since all members depositing or viewing data must do so through predetermined views of the data that are controlled, formatted and presented by view templates running on a DBMS query processor, it is a simple matter to include CKM encrypting and decrypting operations as a part of the database templating process. Thus, when a member requests a specific view of the data, the database references the template selected, reads the credentialing information for each field, fetches the data and encrypts it with the appropriate working key, storing the encrypted Random value within the object header in the normal fashion. The member then retrieves the CKM-encrypted data and uses his/her member profile to access that data for whatever job task is under way.
- A variation on the above approach is to use a single secret symmetric key to encrypt all the data in the database, thus providing protection against hackers that might search the storage medium with sophisticated analytical tools. This inserts a decryption/encryption step into all database access for either internal or external use, but nevertheless is perfectly workable. All CKM credentialing and encrypting operations are still handled by the templating process.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 101 of 115

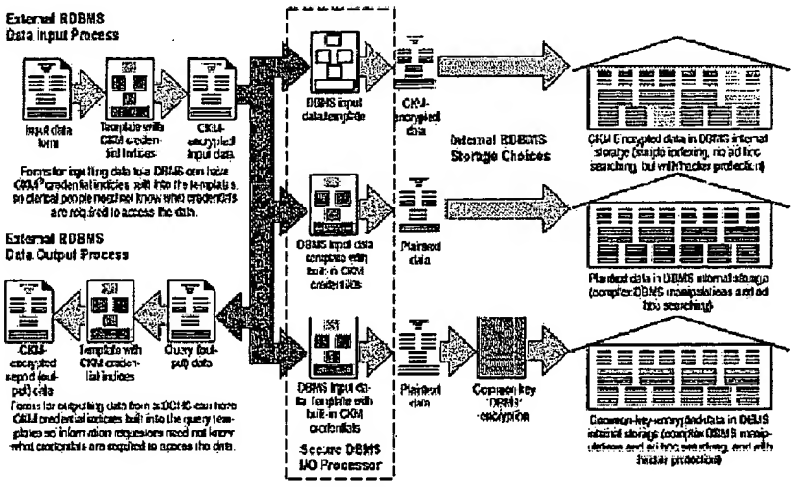


Figure 10. CKM database security choices

Since different organizations have different security policies pertaining to the architecture and management of their databases, there are a number of solutions—and combinations of solutions—available to deal with the database maintenance problem. A number of large Federal agencies are currently working with the major database and template companies to perfect the most optimum ways of storing and retrieving CKM-enabled data to and from Federal databases. Undoubtedly newer and better variations will continue to evolve as these organizations gain more experience in deploying CKM-enabled systems.

A major advantage of CKM is that many people with different data access rights may all request and obtain the same standard database input or query form over the network. Since different data fields may have different credentials applied to them, only the information appropriate to each member is made available to that member. This allows a single database system to serve the needs of potentially thousands of people, each inputting or outputting only data related to their job roles, but with all members sharing a standard set of templated forms and the same (non-duplicated) data repository.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 102 of 115

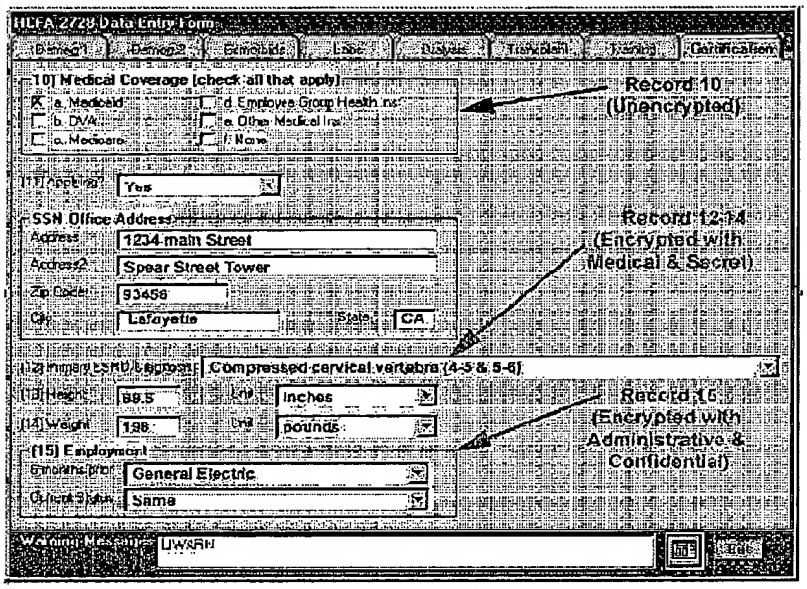


Figure 1.1. An example of a database query form encrypted with multiple credential sets.

4. Member Profile Storage Choices

4.1 The Smart Card—A Decentralized Profile Storage Scheme

A smart card is a thin piece of plastic the size of a credit card but with a processor, read/write memory, and metal contacts so that Input/Output (I/O) can take place. ISO 7816 provides the specification for smart cards. A CKM-enabled Smart Token card stores Member Profiles. I/O between an ISO smart card and a workstation can be relatively slow, making session logon relatively lengthy. Nevertheless, with the greater storage and processing capability becoming available today, smart cards hold much promise for secure, portable information storage, as well as possessing the advantage of three-factor security (something you know (a PIN), plus something you have (the smart card), plus something you are (biometrics)).

Secure storage in the case of a Smart Token card means that data is either stored in a secure area of memory that can only be accessed by the smart card operating system, or data is encrypted with keys stored in a secure area of memory.

Figure 12: An example of a Smart Token card

Smart cards are a secure and portable CKM profile storage option. They hold a member's profile information and the critical encryption algorithms, and are removed from the system (card reader) and secured on the person when the member does not wish to be on-line. This makes it extremely difficult for attackers to hack into the security system since:

- Credentials (member profile) and critical crypto algorithms such as sign and verify and key assembly (combiner) are *not* on the workstation or the workstation's hard drive, but on a secure Smart Token card.
- The network has no access to the smart card in the card reader, and if a smart card is found by an attacker, it will not function without the member's PIN and/or biometric scan data.
- The card allows for portability and flexibility. A member may move from one computing or access device to another and still have appropriate access.

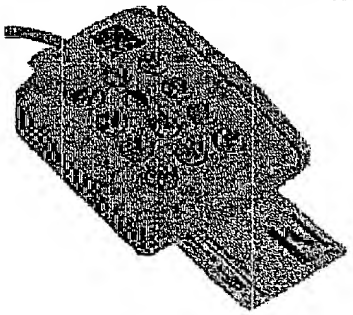


Figure 13. An example of a smart card reader with integral PIN pad.

CrypTEC Systems and TECSEC Incorporated are currently developing a secure smart card with enhanced storage and processing, as well as hardware random number generation capability,

asymmetric key pair generation, and tamper detection. This smart card is called the Smart Token card. It currently uses a smart card micro-controller with 32KB of EEPROM memory, 32KB of ROM memory, and an attached crypto coprocessor. It will eventually use up to a 32-bit processor and carry several megabytes of storage. The crypto coprocessor performs large number math and bit manipulation very rapidly, substantially improving the processing speed of cryptographic algorithms. Certain areas of memory will only be readable by the card operating system, thus protecting keying material. Since Member Profiles and the CKM processes that create working keys will reside on the card, only session logon information and working keys for large objects need to be exchanged via card I/O. Larger profile files need to be communicated across the card I/O only during profile installation and activation, so the smart card bandwidth limitations are not a system performance factor.

Another feature being developed is the inclusion of a biometric capability. This capability with a smart card would allow a high level of security with strong UID, as well as the ability to store different types of information about the member in a package that is easy to carry and easy to use. At present, several fingerprint devices are available on the market, as well as facial recognition, speech recognition, and lip movement recognition devices.

4.2 The Ulogon .com Web Service—A Centralized Member Profile Scheme

An alternative to the approach of utilizing smart cards and readers at each desktop to contain a member's profile is to place that profile on a secure web server, and access it when needed via the Internet. With this approach, the smart card and reader may be eliminated from the system, and CKM functionality can essentially be rented on a month-by-month or week-by-week basis.

The ULogon model essentially moves the smart card functions to a secure ULogon server, using a profile unique to the user and the domain(s) he/she belongs to. The desktop still would encrypt and decrypt files, and would rely upon the ULogon server for signing and verifying and all working key creation. The server would hold all private keys and certificates, the user's CKM profile, including credentials, and the Biometric templates. The server will have a "member profile" for each user and administrators will simply transmit credentials and other periodic maintenance details to users via their server-based mailbox instead of via email. Domain and Workgroup Administrators will perform their administrative chores via connection to the ULogon web site, instead of on their local systems.

Since the wire connecting the ULogon server-based user profile (containing the equivalent of the smart card) is now quite long (the Internet) and vulnerable to attack, Diffie-Hellman key exchange routines are used by both the server and the desktop, so the desktop and server can exchange private information securely, such as working keys, command requests, message digests to be signed, etc. This means that a user will need to have a reliable connection to the ULogon server, since every time an object needs signing or verifying, or every time a working key needs to be constructed to create or access an encrypted object, the server will have to be engaged. This also means that if the server or the network goes down, the user is temporarily out of work.

However, there are some advantages to the centralized ULogon approach, including:

1. Lower costs of entry for the customer; instead of paying, say $50–$100/seat for the CKM software license and $50/seat for a CDROM, smart card and reader, the user can now pay a smaller monthly rate, say, $8-10/seat/month

2. Mobility; A user can now travel the web and log in from anywhere. (He may need to drag a video camera and microphone and a CD around with him if he uses BioID, which uses facial, voice and lip movement as biometric authentication modes.)

3. Convenience; the big expense in deploying CKM is not the cost per seat or the card and reader, but rather the training and systems integration work necessary to setting up the infrastructure—especially training Domain Authorities and Workgroup Administrators. Thus, a central web-based approach can provide a lot of convenience, including:

- A professional and readily accessible training tool (access the site for training programs)
- An easy way to download necessary user and administrative software modules
- An easy way to set up and maintain domain and workgroup administrative functions
- No smart card hardware to install or debug
- Larger and more numerous domains and biometric templates can be managed (no smart card memory constraints)
- Using BioID, member enrollment will be much easier since it can be carried out on-line via a video/audio/keyboard chat interview using the BioID for authentication. Enrollees can even hold their passports or drivers licenses up to the camera.
- Guest users and pilot tests can be created overnight
- The bureaucratic hassle associated with setting up a new (CKM-based) security access control system within a large company can be avoided, since the web-hosted CKM service is "self-contained," easy to acquire and use, and can be purchased by lower management budget authority.

4. Better security

- Using BioID, users can be authenticated better (use both BioID and passwords for better security), since passwords are easier to defeat and users can give them to each other if they wish
- WebCKM has substantially less potential for illegal surreptitious access to administrative systems during off hours, better authentication of the administrator, and much reduced requirements for physical security.
- WebCKM has rapid response to maintaining users and foiling security attacks (can change anyone's status immediately and thus reduce the risk of rogue users)

The Centralized Smart Card Model

A variation on the centralized server model is to use smart cards or other tokens at each desktop, and yet require each user to log in to a central server once a day to be synchronized with the centrally-maintained credentials files and to utilize the BioID authentication to the smart card. If a user has additional needs for Ulogon's Virtual Presence or Virtual Interactivity services, then logging in every day will become a normal part of the work schedule.

5. The Power of CKM: Solutions

Cryptography and its related elements are generally viewed as merely a utility, the sole purpose of which is to provide security and confidentiality to data and voice storage and communications. This is true of most cryptographic key management schemes and encryption software applications. However, it is not true for CKM. The ability to selectively encrypt objects within objects and the granting of role-based access to these objects sets CKM apart from other key management methods. CKM attributes provide the basis for solving business communications problems in uniquely beneficial ways.

One-to-Many Distribution

CKM allows for a one-to-many distribution of encrypted objects where the creator does not know the identity and related access rights of the many, including future members within the domain. This provides the basis for secure broadcast of sensitive material. Secure CKM one-to-many distributions can be used for numerous corporate, employee, medical, customer, and vendor applications.

Dynamic Data Separation

CKM separates data cryptographically. Each set of credentials used within a domain separate that data from all other data within the domain. This data separation is enforced cryptographically, and not by separate physical architectures. With CKM, data separation—including layers within layers (objects within objects)—can be dynamically changed to meet organizational requirements regarding information flow and access boundaries. In essence, CKM can provide dynamic, cryptographically enforced private networks within a larger organizational network.

Distinct Separate Reality

CKM can take one or more encrypted objects and encrypt them within another encrypted object. It is this object-within-an-object that provides CKM with the ability to selectively decrypt objects according to access rights previously given to members.

For example, management desires to post a memorandum to all employees on its Intranet web server. In addition, management wishes to include additional confidential information for Managers. With CKM, the portion of the document intended for all employees would be encrypted with credentials every member in the domain possesses. The portion of the document pertaining to management would be encrypted using a credential limited to managers. When employees download and decrypt the document, all employees would view the common information. Managers would also view the restricted information. With CKM, it is possible to have each member view an object or objects and not know their access differs from others.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 107 of 115

Flexible Role and Responsibility Assignment

CKM and the Smart Token do not exist in a vacuum. Other parts of the system reside on the member's desktop computer, and on the administrator's computer system elsewhere on the network. Servers are not required by the CKM architecture, but the architecture will accommodate servers easily in the system if required.

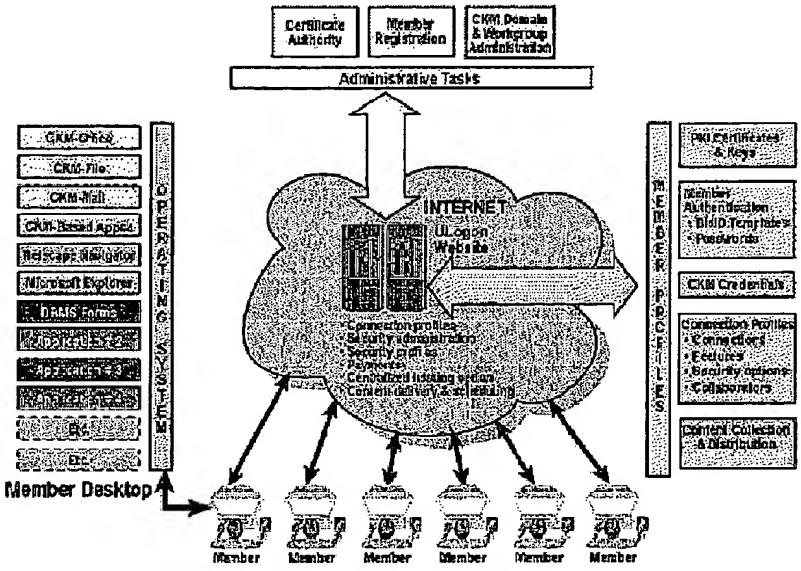


Figure 17. The CKM security layer for a typical web-based system is shown above. It consists of the CKM modules located on the member's personal computer, as well as connections through the Internet to the Ulogon web site for access to the member's keys, certificates and member profile. Another critical set of functions resides on the Ulogon server for the Workgroup Administrator and Domain Authority.

Administrative functions may be separated into as many levels as needed for security and workload needs. Organizations may continue to use the included 3-tier system consisting of a Domain Authority, Workgroup Administrators and Workgroup Members, or they may customize this system for more or less separation of functions and levels of distribution.

Administrative roles and responsibilities are not bound, a priori, to any level or component. If the standard role assignments of Domain Authority, Workgroup Administrator, and Workgroup

Member do not meet an organization's needs, applications may be customized for other assignments. Responsibilities may be moved up or down the distribution hierarchy, or roles may be assigned in a completely different manner.

5.1 The U.S. Postal System and certified electronic mail

The U.S. Government, through several Congressional Acts, has mandated that all required document submissions to all federal agencies must be electronic by March 2003. The anticipated savings to both governments and companies are astronomical, and run into the hundreds of billions of dollars per year. However, just getting the information to the government securely is only part of the problem. The most important part is making that data securely and efficiently available to the people who must access it throughout industry and government.

The United States Postal Service is evaluating a new secure certified electronic mail system for industry and government that will enable the submission of these documents electronically in place of the centuries-old paper method. This system has been called "eProof" internally, but will most likely have the new name of "NetPost.Certify" for formal introduction (anticipated in Summer of 2000).

Through this new certified email service, a corporation sending mandatory data to a Federal agency would do so through the Internet and a USPS smart card. A corporate member would typically possess two sets of credentials—one for the USPS transport process over the Internet, and one corresponding to the domain of the Federal agency the data is being sent to. The data would be broken into objects, each encrypted with a working key protected by a specific set of credentials associated with the agency's domain. If required by the agency, all objects in a particular submission could be "wrapped" (encrypted) again using a broader level of credentials such that only members of that domain could open the complete data package (some of which may have been designated as unencrypted). The encrypted package would then be wrapped again (encrypted) with a set of working keys and credentials associated with the USPS, and the multiply-encrypted package would be sent to the Federal Agency.

Upon receipt of the data package, the agency would "open" (decrypt) the USPS wrapper, send notification of receipt to a USPS server, which would return a date and time-stamped certified notice to both the agency and the submitting corporation (the certified email receipt). Upon receipt of the USPS certification, the agency would open its domain wrapper and send the encrypted objects to wherever they need to reside within the agency for further processing and storage (typically a database management system).

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 109 of 115

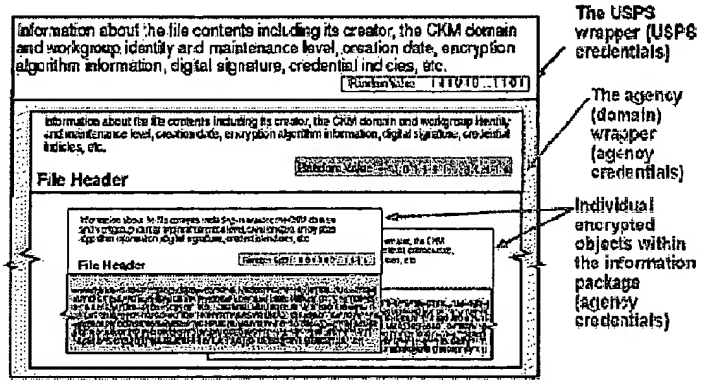


Figure 18. The proposed USPS object hierarchy for a typical data submission to a Federal agency.

All of these data transmissions can take place over the Internet as pieces of electronic mail—quickly, inexpensively, and securely.

The USPS plans to charge less than typical paper-based certified mail for each such transmission. The target markets are business-to-government, state-to-federal-government, and business-to-business. The first major customers for the service are anticipated to be the IRS, the Social Security Administration and the Health Care Financing Administration, which processes Medicare/Medicaid data on behalf of 75 million Americans.

The USPS—the only commercial entity in the US that can issue electronic credentials for e-commerce for which the penalty for tampering is a federal felony—would provide and maintain the infrastructure for certified email usage, principally consisting of the readers and smart cards and desktop software for members, as well as the administrative CKM functionality for government agencies and corporations. The USPS would also provide the certificate authority for issuing certificates to members, as well as the smart card initialization and personalization functions necessary for registering new members and issuing cards to them.

CKM is the necessary USPS technology that provides the secure fine-grained differentiated access to authorized information users within the government and corporate worlds. Smart cards with CKM-enabled functionality are essential to this service. Currently, the USPS is negotiating a multi-year contract with TECSEC to design and implement the new secure electronic USPS system using CKM technology.

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 110 of 115

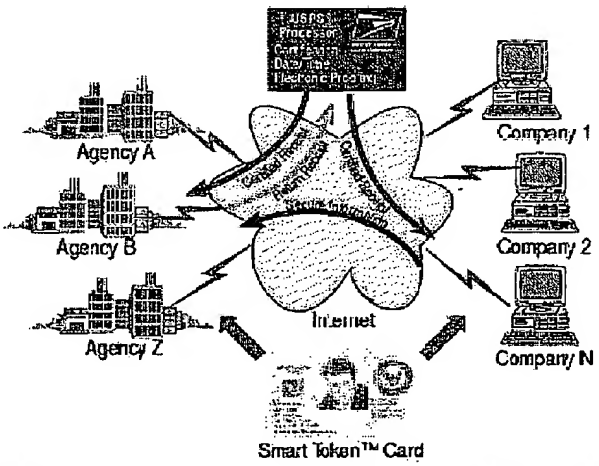


Figure The USPS certified email system would deliver secure certified email to government agencies and return a receipt of delivery.

Other government agencies are also evaluating the "NetPost.Certify" system over time for their document submissions from the commercial world.

Once the industry-to-government and government-to-government document transfer system is up and running, the USPS could take this service to the world as a company-to-company service, and ultimately as a consumer-to-consumer service. Other post office agencies in many countries are already interested in adopting this technology, and many may follow the USPS's lead and offer similar or identical services in their countries. Since CKM crypto is exportable around the world, there should be no legal or national security issues involved in rapidly expanding USPS/CKM technology to the rest of the world. Obviously, adoption of this CKM-enabled technology by the world's post offices would establish CKM as a de facto as well as official standard for secure, exportable, certified access to information.

6. Conclusion

CKM is a powerful key management technology that has substantial advantages over other more conventional key management systems. CKM is flexible and may exist with and use the strong attributes of public key infrastructures, such as identification and authentication, to form a superior combined key management and encryption system.

CKM brings substantial advantages to organizations, including:

- Distributed role-based access control: CKM's distributed role-based access control, one-to-many distribution and data separation characteristics allow organizations to tailor their crypto security to suit the way their information is created, distributed, consumed and stored—a much better solution than the centralized, one-to-one nature of traditional public key cryptosystems.
- Fine-grained access: CKM allows documents and files to be split up into separate objects, and objects may have other objects within them. This capability allows different parts of a document or file to each require different credentials for access, and thus allows organizations to precisely map information access to the way in which the information naturally flows within the day-to-day workflow.
- Key recovery: CKM's architecture makes it possible for Domain Authorities to provide access to encrypted files for which the key values have been lost by members. This has two benefits: (1) organizations can encrypt their critical information without fear of loss due to lost keys; and (2) CKM satisfies the emergency access needs of criminal investigation and national security authorities (a court order can compel a workgroup administrator to recreate the necessary keys), and is thus easily exportable around the world.
- Versatility: CKM is extremely flexible, and is compatible with traditional public key infrastructures, and can be implemented with smart cards to hold member profiles, or with a WebCKM server (Ulogon.com). Alternatively, CKM can be used without a PKI, and still remain flexible and scalable.
- Industry standard: CKM is an ANSI X9.69 standard, and may soon be deployed by the US Postal Service for a new secure certified electronic mail system that will be used by government and industry to enable true paperless communications. Since postal systems must be compatible around the world, other nations may also be adopting CKM-based electronic postal services. This would make CKM a worldwide de facto standard that will insure its presence for some time to come.
- Performance and Scalability: Public key crypto has a debilitating effect on a computer performance, and centralized security/permissions servers typically end up becoming resource intensive bottlenecks, as well as single points of failure. CKM's crypto uses public key crypto very sparingly, and the normal symmetric working key encryption processing is executed on the members' desktop computer, and not on a centralized security or permissions server. This means that CKM crypto is hundreds of times faster than traditional public key-based crypto systems, and performance bottlenecks are not likely to appear in the system, no matter how large it becomes.

A flexible key management architecture would ideally support symmetric encryption, Public Key Infrastructures, and CKM. These three technologies, blended together properly, can meet all of the requirements of secure electronic commerce around the world. This kind of encryption can effectively address emerging privacy and liability issues. The closed domain nature of an established CKM encryption boundary within a business interest can separate data effectively and easily delineate liability.

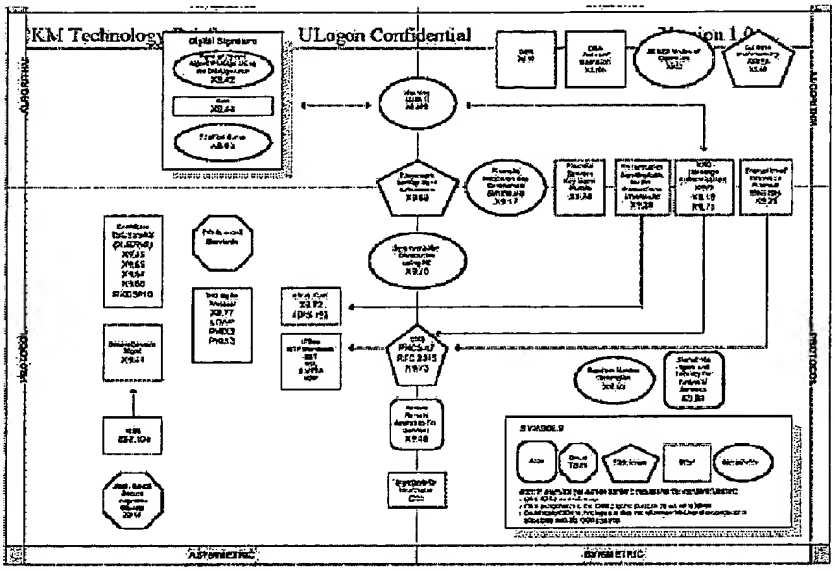
Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

A business can now select key management methods that more closely reflect their security needs. The response to these demands focuses more on selecting the proper mix rather than selecting between competing encryption technologies.

The fine-grained, object-based encryption capability of CKM provides confidentiality to the millions of objects in an organizational database of information, and allows large organizations to put their mission-critical information assets directly on the network for even more efficient access by their thousands of employees, partners, vendors and customers. This in turn allows a complete severing of the dependence on paper-based information transmittal and storage, which in turn will finally lead us into a true electronic commerce future.

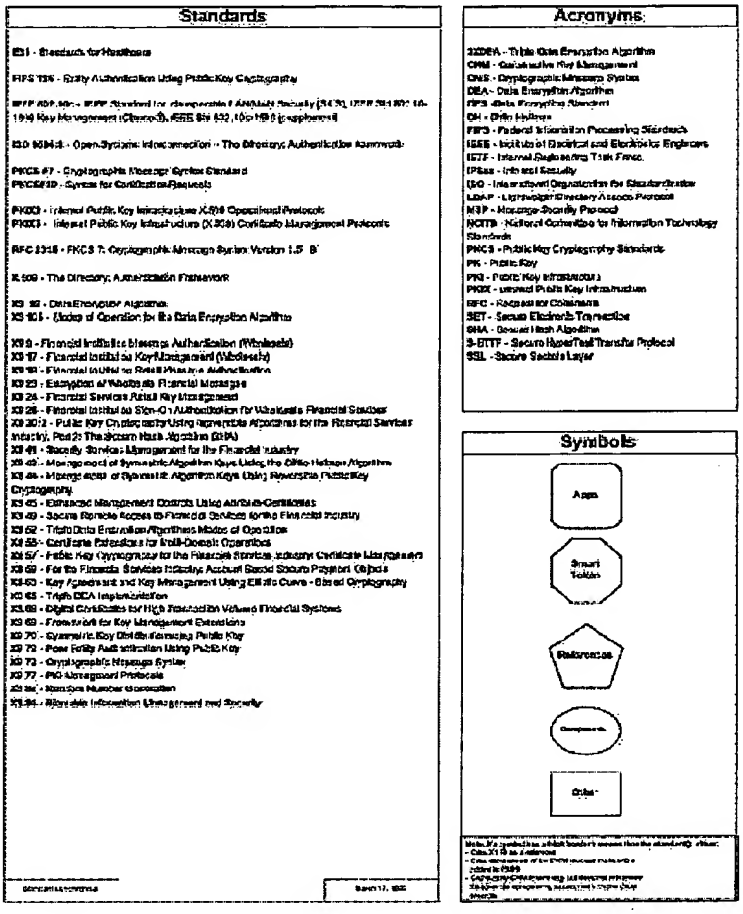
Appendix A: Standards

Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT



Declaration under 37 C.F.R. § 1.131
Applicants: William B. Sweet et al.
Serial No.: 09/930,029
Filed: August 14, 2001
Docket No.: 055120-0002
Title: METHOD AND APPARATUS FOR A WEB-BASED APPLICATION SERVICE MODEL FOR SECURITY MANAGEMENT

Page 114 of 115



Appendix B: Export Considerations

The White House recently announced a relaxation of US encryption export policy. Although specific regulations have not been issued, the following rules are anticipated:

After a one time review and approval, "commercial" encryption products with any key length may be exported without restriction to customers in most countries. There are some restricted country destinations, mostly for national security reasons. An annual reporting to the US Department of Commerce listing the identity of foreign purchasers may be required. See the Department of Commerce, Bureau of Export Control, http://www.bxa.doc.gov/Encryption/Default.htm on the web for further detail.

Since CKM encryption technology features 100% key recovery by the system owner, TESCEC has been granted an unrestricted export license for its CKM-2000 product line—except to prohibited country destinations. TECSEC's CKM-2000 family of products uses Triple DES algorithms and up to 392-bit (symmetric) key length. Based on CKM's 100% key recovery feature, it is believed that future CKM products, after one-time product reviews, may be exported with any key length and any algorithm.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.